Dell Encryption Key Manager 3.0
Bereitstellungshandbuch

Anmerkungen, Vorsichtshinweise und Warnungen

ANMERKUNG: Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie den Computer besser einsetzen können.

VORSICHT: Ein VORSICHTSHINWEIS macht aufmerksam auf mögliche Beschädigung der Hardware oder Verlust von Daten bei Nichtbefolgung von Anweisungen.

WARNUNG: Durch eine WARNUNG werden Sie auf Gefahrenquellen hingewiesen, die materielle Schäden, Verletzungen oder sogar den Tod von Personen zur Folge haben können.

Irrtümer und technische Änderungen vorbehalten.

© 2011 Dell Inc. Alle Rechte vorbehalten. Gedruckt in den USA.

Die Vervielfältigung oder Wiedergabe dieser Unterlagen in jeglicher Weise ohne schriftliche Genehmigung von Dell Inc. ist strengstens untersagt.

In diesem Text verwendete Marken: Dell™, das Dell Logo, Dell Precision™ , OptiPlex,™ Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™ und Vostro™ sind Marken von Dell Inc. Intel®, Pentium®, Xeon®, Core® und Celeron® sind eingetragene Marken der Intel Corporation in den Vereinigten Staaten und anderen Ländern. AMD® ist eine eingetragene Marke und AMD Opteron™, AMD Phenom™ und AMD Sempron™ sind Marken von Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS ®und Windows Vista® sind Marken oder eingetragene Marken der Microsoft Corporation in den Vereinigten Staaten und/oder anderen Ländern. Red Hat® und Red Hat® Enterprise Linux® sind eingetragene Marken von Red Hat, Inc. in den Vereinigten Staaten und/oder anderen Ländern. Novell® ist eine eingetragene Marke und SUSE® ist eine Marke von Novell Inc. in den Vereinigten Staaten und anderen Ländern. Oracle® ist eine eingetragene Marke von Oracle Corporation und/oder ihren Tochterunternehmen. Citrix,® Xen,® XenServer® und XenMotion® sind eingetragene Marken oder Marken von Citrix Systems, Inc. in den Vereinigten Staaten und/oder anderen Ländern. VMware,® Virtual SMP®, vMotion,® vCenter® und vSphere® sind eingetragene Marken oder Marken von VMWare, Inc. in den Vereinigten Staaten oder anderen Ländern. IBM® ist eine eingertragene Marke von International Business Machines Corporation.

Andere in diesem Dokument möglicherweise verwendete Marken und Handelsnamen beziehen sich auf die entsprechenden Eigentümer oder deren Produkte. Dell Inc. erhebt keinen Anspruch auf Marken und Handelsbezeichnungen mit Ausnahme der eigenen.

2011 – 12

Rev. A00

Inhaltsverzeichnis

Anmerkungen, Vorsichtshinweise und Warnungen....2

Kapitel 1: Übersicht....5
Hardware- und Software-Anforderungen....6
Server-Hardwareanforderungen....6
Browser-Anforderungen....6
Betriebssystem-Anforderungen....6

Kapitel 2: EKM 3.0-Installation....7
Vorbereitung der Installation von EKM 3.0 in Microsoft Windows....7
Vorbereitung auf die Installation von EKM 3.0 in Red Hat Enterprise Linux....8
PVorbereitung auf die Installation von EKM 3.0 in SUSE Linux Enterprise Server....8
Durchführung des EKM 3.0 Installationsverfahrens....9

Kapitel 3: Einrichtung von primären und sekundären EKM 3.0-Servern....13
Installation von EKM 3.0 auf dem primären Server....13
Verwendung von EKM 3.0 auf dem primären Server....13
Installation von EKM 3.0 auf dem sekundären Server....13
Verwendung von EKM 3.0 auf dem sekundären Server....14
Deinstallation von EKM 3.0 von den primären und sekundären Servern....14

Kapitel 4: Durchführung von Sicherungen und Wiederherstellung aus einer Sicherung....15
Erstellung einer Sicherung des Keystores....15
Wiederherstellung aus einer Sicherung 16

Kapitel 5: EKM 3.0 - Verwendung....17
Anmeldung am Encryption Key Manager 3.0 Portal....17
Erstellung eines Master-Keystores 18
Aktivieren der Firewall in EKM 3.0 Server....18
Konfigurieren von EKM 3.0 zum Akzeptieren von Geräten, die EKM 3.0 kontaktieren, um Schlüssel zu erhalten....19
Erstellen einer Gerätegruppe....19
Erstellung von Schlüsselgruppen für eine Gerätegruppe....20
Hinzufügen eines Gerätes zu einer Gerätegruppe....21
Hinzufügen und Löschen von Schlüsseln aus Schlüsselgruppen....21
Löschen von Schlüsselgruppen....22
Überprüfung des Serverzertifikats....23

Anzeigen der Serverzertifikateinzelheiten....23
Anmeldung am WebSphere-Server....24
Starten und Stoppen des EKM 3.0 Servers in Windows....24
Starten und Anhalten des EKM 3.0 Servers in Linux....24

Kapitel 6: Migration und Zusammenführung....27
Migration einer Encryption Key Manager (EKM) 2.X-Version während der EKM 3.0-Installation....29
Migrationsverfahren für EKM 2.X auf EKM 3.0....29
Zusammenführung von Encryption Key Manager (EKM) 2.X in EKM 3.0 nach der Installation von EKM 3.0....31
Zusammenführungstool-Voraussetzungen....33
EKM 2.X auf EKM 3.0 Zusammenführungsverfahren....33
Überprüfen der EKM 2.X auf EKM 3.0 Zusammenführung oder Migration....37
Zusammenführungsfehler....38
Zusammenführung von zusätzlichen EKM 2.X Versionen mit EKM 3.0....38
Löschen des ekmcert-Zertifikats, der Schlüssel und Schlüsselgruppen und Umbenennen von Geräten....39

Kapitel 7: Deinstallation von EKM 3.0....45
Deinstallation von EKM 3.0 unter Windows....45
Deinstallation von EKM 3.0 in Linux....46

Kapitel 8: Fehlerbehebung....47
Kontaktaufnahme mit Dell....47
Überprüfungen der Systemvoraussetzungen....49
Fehlercodes....51
Windows Referenzdateien....53
Linux-Referenzdateien....55
Manuelle Deinstallation von EKM 3.0....57
Manuelle Deinstallation von EKM 3.0 in Windows....57
Manuelle Deinstallation von EKM 3.0 in Linux....58
Erneutes Installieren von EKM 3.0....59
Häufig gestellte Fragen (FAQs)....59
Bekannte Probleme und Lösungen....62
Installieren der compat-libstdc++ Library....65

1

Übersicht

Dell Encryption Key Manager (EKM) 3.0 ist ein Verschlüsselungsdienstprogramm, dass die auf LTO-Bandkassetten gespeicherten Daten absichert, indem es Verschlüsselungscodes für Dell Band-Automatisierungslösungen verwaltet, einschließlich der ML- und TL PowerVault-Reihen. EKM 3.0 verwaltet den Lebenszyklus von Bandverschlüsselungscodes, einschließlich der Erstellung, Verteilung, Verwaltung und Löschung.

Diese Anleitung beschreibt Installation, Konfiguration und das Durchführen von grundlegenden Vorgängen in Dell Encryption Key Manager 3.0 (EKM 3.0). Dell empfiehlt, dass Sie dieses Dokument lesen, bevor Sie EKM 3.0 installieren.

Diese Anleitung enthält Informationen zu folgenden Themen:

- Hardware- und Softwareanforderungen für EKM 3.0
- Installation und Deinstallation von EKM 3.0 auf den Plattformen Windows und Linux
- Konfiguration von EKM 3.0
- Grundlegende Vorgänge in EKM 3.0
- Migration von EKM 2.X während der EKM 3.0-Installation und Zusammenführung von EKM 2.X mit einer konfigurierten EKM 3.0-Installation
- Häufig gestellte Fragen (FAQs), Fehlerbehebungsinformationen, allgemeine Fehlermeldungen und Kontaktinformationen für den Dell Support.

ANMERKUNG: EKM 3.0 basiert auf IBM Tivoli Key Lifecycle Manager (TKLM) V2 FixPack 2, wurde jedoch durch Auswahl des entsprechenden Subsets der TKLM-Band-Funktionen für die Unterstützung von Dell Band-Library-Umgebungen angepasst.

Informationen zur Verwendung von EKM 3.0 sind in dieser Anleitung nicht enthalten, beziehen Sie sich hierfür auf die TKLM-Dokumentation, in der die folgenden Themen enthalten sind:

- IBM Tivoli Key Manager 2.0 *Schnellstart-Handbuch*
- IBM Tivoli Key Manager 2.0 *Installations- und Konfigurationshandbuch*
- IBM Tivoli Key Manager 2.0 *Produktübersicht/Szenariohandbuch*

Lesen Sie für Informationen zum Zugriff auf die TKLM-Dokumentation den Abschnitt „Dokumentation und Referenzmaterialien“ der Datei **ReadThisFirst.txt** auf dem EKM 3.0 Installationsdatenträger.

Einige in der IBM TKLM-Dokumentation beschriebenen Bildschirme und Funktionalitäten sind in Dell EKM 3.0 nicht aktiviert. EKM 3.0 enthält nur eine Untermenge an Funktionen, die zur Unterstützung von Dell PowerVault Band-Libraries benötigt werden.

ANMERKUNG: Beziehen Sie sich für die empfohlene Verwendung und Konfiguration von Dell EKM 3.0 auf den Abschnitt „Bewährte Verfahren“ der Datei **ReadThisFirst.txt** auf dem EKM 3.0 Installationsdatenträger.

ANMERKUNG: Beziehen Sie sich für die neuesten Informationen, einschließlich Funktionsverbesserungen und Fehlerbehebungen (Bugfixes) auf die Versionshinweise auf: **support.dell.com/manuals**. Navigieren Sie zu **Software → Systems Management → Dell Encryption Key Manager** .

Hardware- und Software-Anforderungen

Server-Hardwareanforderungen

Die minimalen Hardwareanforderungen für den Key Management Server (die Hardware, auf der EKM 3.0 installiert wird) sind:

- CPU: 2.3 GHz
- Speicher: 4 GB ECC-Speicher
- Verfügbarer Festplattenspeicher (für EKM 3.0-Installation und typischen Schlüsselspeicher): 5 GB

ANMERKUNG: Wenn das System, auf dem Sie EKM 3.0 installieren 24 oder mehr CPUs hat, dann beziehen Sie sich auf die EKM 3.0 Versionshinweise, um Einzelheiten zur Aktualisierung von EKM 3.0 nach Abschluss der Installation zu erhalten. Gehen Sie für den Zugriff auf die EKM 3.0 Versionshinweise auf **support.dell.com/manuals** und navigieren Sie zu **Software → Systems Management → Dell Encryption Key Manager**.

Browser-Anforderungen

EKM 3.0 unterstützt die folgenden Browser:

- Microsoft Internet Explorer, Version 7.0
- Microsoft Internet Explorer, Version 8.0, Kompatibilitätsansichtsmodus
- Firefox Version 3.0.x (EKM 3.0 unterstützt Firefox Version 3.5 und höher nicht.)

ANMERKUNG: JavaScript muss aktiviert sein, damit alle EKM 3.0 Funktionen funktionieren. Beziehen Sie sich auf die Dokumentation Ihres Browsers, um Anweisungen zum Aktivieren von JavaScript zu erhalten.

Betriebssystem-Anforderungen

EKM 3.0 unterstützt die folgenden Betriebssysteme:

- Windows Server 2003 R2 mit Service Pack 2, 32- und 64-Bit, Standard und Enterprise Edition
- Windows Server 2008 mit Service Pack 2, 32- und 64-Bit, Standard und Enterprise Editione
- Windows Server 2008 R2, Standard und Enterprise Edition
- Red Hat Enterprise Linux (RHEL) 4.X, Advanced Server (AS), 32-Bit
- Red Hat Enterprise Linux (RHEL) 5.X, 32- und 64-Bit
- SUSE Linux Enterprise Server (SLES) 10 mit Service Pack 4, 64-Bit
- SUSE Linux Enterprise Server (SLES) 11 mit Service Pack 1, 64-Bit

ANMERKUNG: EKM 3.0 unterstützt kein VMware bzw. Microsoft Hyper-V Server.

ANMERKUNG: Beziehen Sie sich für Informationen zu den Anforderungen und Einschränkungen bei der Einrichtung eines primären / sekundären Servers auf Einrichtung der primären und sekundären EKM 3.0 Server.

ANMERKUNG: EKM 3.0 führt vor der Installation Vorüberprüfungen durch. Beziehen Sie sich für weitere Informationen auf System-Vorüberprüfungen.

2

EKM 3.0-Installation

Dieses Kapitel beschreibt die Installation von EKM 3.0 unter Windows und Linux.

ANMERKUNG: Wenn Sie derzeit EKM 2.X verwenden, empfiehlt Dell die Beibehaltung Ihrer derzeitigen Infrastruktur (durch EKM 2.X geschützte Server, Betriebssysteme, Band-Libraries, etc), wenn keine Probleme auftreten.

EKM 3.0 unterstützt keine Virtual Machines als Hosts. Wenn Sie eine Virtual Machine als Ihren EKM 2.X-Host verwenden, müssen Sie auf EKM 2.X bleiben, oder auf einen physikalischen Server migrieren.

ANMERKUNG: Wenn Sie EKM 2.X auf EKM 3.0 migrieren wollen, dann beziehen Sie sich auf Migration einer Encryption Key Manager (EKM) 2.X Version während der Installation von EKM 3.0, bevor Sie mit der EKM 3.0-Installation beginnen.

ANMERKUNG: Dell empfiehlt, dass Sie EKM 3.0 auf einem dedizierten Server installieren, der für keine anderen Dienste verwendet wird. Dies stellt sicher, dass die Leistung und Reaktionszeit von EKM 3.0 nicht durch etwaige anderen Anwendungen beeinträchtigt wird, die auf dem gleichen physikalischen Serber ausgeführt werden.

VORSICHT: EKM 3.0 unterstützt nur die direkte Installation vom EKM 3.0-Datenträger aus. Kopieren Sie die Inhalte des EKM 3.0-Datenträgers nicht auf Ihre Festplattte.

ANMERKUNG: Die Verfahren in diesem Kapitel erfordern Kenntnisse auf Administratorebene.

Vorbereitung der Installation von EKM 3.0 in Microsoft Windows

Dieses Kapitel beschreibt die Schritte vor der Installation für Dell Encryption Key Manager 3.0 in Microsoft Windows.

ANMERKUNG: Das Installationsverfahren nimmt etwa 45 Minuten in Anspruch. Schalten Sie das System nicht aus, bevor die Installation abgeschlossen wurde.

ANMERKUNG: Sie müssen für die Installation von EKM 3.0 als **Administrator** angemeldet sein.

ANMERKUNG: Wenn Sie für die Datenbank kein komplexes Kennwort verwenden wollen, dann deaktivieren Sie im Betriebssystem die Einstellung **Kennwort muss Komplexitätsvoraussetzungen erfüllen**, bevor Sie den EKM 3.0 Installationsdatenträger einlegen.

1. Legen Sie die EKM 3.0 für Microsoft Windows Installations-DVD in das System ein, auf dem Sie EKM 3.0 installieren wollen.
2. Wenn Ihr System für die automatische Ausführung bei Einlegen einer DVD eingestellt ist, dann warten Sie einen Moment, bis das Installationsprogramm angezeigt wird. Wenn Ihr System nicht für die automatische Ausführung eingestellt ist, dann navigieren Sie zum DVD-Laufwerk und doppelklicken Sie auf das DVD-Laufwerk, oder die **install.exe** im Stammverzeichnis des DVD-Laufwerks.

   Es wird der **Begrüßungsbildschirm** des EKM 3.0 Installationsassistenten angezeigt.

ANMERKUNG: Wenn Sie EKM 3.0 über eine Netzwerkfreigabe installieren wollen, dann verwenden Sie keinen Pfad im Format: **\\<*IP_Adresse*>*EKM_3.0_Freigabe***. Weisen Sie der Freigabe stattdessen einen Laufwerksbuchstaben zu. Verwenden Sie im Windows Explorer **Extras** → **Netzlaufwerk zuordnen**, um den Installationspfad zu **<*Laufwerksbuchstabe* eines freigegebenen Laufwerks>:\<*EKM_3.0_Datenträger*> zu machen**.

Fahren Sie fort mit Durchführung des EKM 3.0 Installationsverfahrens.

Vorbereitung auf die Installation von EKM 3.0 in Red Hat Enterprise Linux

Dieses Kapitel beschreibt die Schritte vor der Installation für Dell Encryption Key Manager 3.0 in Red Hat Enterprise Linux.

ANMERKUNG: Das Installationsverfahren nimmt etwa 45 Minuten in Anspruch. Schalten Sie das System nicht aus, bevor die Installation abgeschlossen wurde.

Führen Sie für die Vorbereitung der Installation von EKM 3.0 die folgenden Schritte durch:

1. Legen Sie den Ihrem Betriebssystem entsprechenden EKM 3.0 Installationsdatenträger in das System ein, auf dem Sie EKM 3.0 installieren wollen.
2. Wenn Ihr System für die automatische Ausführung bei Einlegen einer DVD eingestellt ist, dann warten Sie einen Moment, bis das Installationsprogramm angezeigt wird. Wenn Ihr System nicht für die automatische Ausführung eingestellt ist, dann öffnen Sie ein Terminal mit Root-Zugriff und navigieren Sie in den Ordner, in dem die EKM 3.0 DVD gemountet wurde. Geben Sie **./autorun.sh** ein und drücken Sie **Eingabe**.

ANMERKUNG: Wenn SELinux installiert und aktiviert ist, dann deaktivieren Sie es, bevor Sie die Installation starten. Beziehen Sie sich auf Überprüfungen der Systemvoraussetzungen.

ANMERKUNG: Auf Red Hat-Betriebssystemen wurde oft das **noexec** Bit eingestellt, um die Ausführung von Binärdateien auf den gemounteten Dateisystemen zu deaktivieren. Wenn das **noexec** Bit auf dem gemountetem DVD ROM auf **deaktiviert** eingestellt wurde, dann wird das EKM 3.0-Installationsprogramm nicht von der DVD aus gestartet. Führen Sie die folgenden Schritte durch, um das EKEKM 3.0-Installationsprogramm nicht von der DVD aus zu starten:

a) Öffnen Sie eine Terminalsitzung mit Root-Zugriff.
b) Unmounten Sie die EKM 3.0 DVD.
c) Mounten Sie die EKM 3.0 DVD **schreibgeschützt**, mit deaktiviertem **noexec** neu, indem Sie die folgenden Befehle eingeben:

```
mkdir /media/dellmedia mount /dev/<EKM 3.0 Gerät><space>/media/dellmedia
cd /media/dellmedia
```

d) Geben Sie zum Ausführen des Installationsprogramms **./autorun.sh** ein und drücken Sie **Eingabe**.

Es wird der **Begrüßungsbildschirm** des EKM 3.0 Installationsassistenten angezeigt.

Fahren Sie fort mit Durchführung des EKM 3.0 Installationsverfahrens.

PVorbereitung auf die Installation von EKM 3.0 in SUSE Linux Enterprise Server

Dieses Kapitel beschreibt die Schritte vor der Installation für Dell Encryption Key Manager 3.0 in SUSE Linux Enterprise Server (SLES).

ANMERKUNG: Das Installationsverfahren nimmt etwa 45 Minuten in Anspruch. Schalten Sie das System nicht aus, bevor die Installation abgeschlossen wurde.

Führen Sie für die Vorbereitung der Installation von EKM 3.0 die folgenden Schritte durch:

1. Legen Sie den Ihrem Betriebssystem entsprechenden EKM 3.0 Installationsdatenträger in das System ein, auf dem Sie EKM 3.0 installieren wollen.
2. Wenn Ihr System für die automatische Ausführung bei Einlegen einer DVD eingestellt ist, dann warten Sie einen Moment, bis das Installationsprogramm angezeigt wird. Wenn Ihr System nicht für die automatische Ausführung

eingerichtet wurde, dann öffnen Sie ein Terminal mit Root-Zugriff und navigieren Sie in den Ordner, in dem die EKM 3.0 DVD gemountet wurde. Geben Sie **./autorun.sh** ein und drücken Sie **Eingabe**.

Es wird der **Begrüßungsbildschirm** des EKM 3.0 Installationsassistenten angezeigt.

ANMERKUNG: Wenn SELinux installiert und aktiviert wurde, dann deaktivieren Sie es vor dem Starten der Installation.

3. Öffnen Sie Port 50000. Führen Sie dafür die folgenden Schritte durch:
   a) Navigieren Sie zu **Computer** → **Places** → **File System** .
   b) Doppelklicken Sie **etc**.
   c) Doppelklicken Sie **Services**.
   d) Ändern Sie in der Datei **Services 50000/tcp** und **50000/udp** auf **50100/tcp** und **50100/udp**.
   e) Klicken Sie auf **Save**.

Fahren Sie fort mit Durchführung des EKM 3.0 Installationsverfahrens.

Durchführung des EKM 3.0 Installationsverfahrens

Dieses Kapitel beschreibt die Installation von EKM 3.0

ANMERKUNG: Das Installationsverfahren nimmt etwa 45 Minuten in Anspruch. Schalten Sie das System nicht aus, bevor die Installation abgeschlossen wurde.

ANMERKUNG: Wenn Sie EKM 3.0 auf einem Server installieren, der als Sekundärserver verwendet wird, müssen die Kennwörter die gleichen Kennwörter sein, die Sie für die Installation des primären EKM 3.0-Servers verwendet haben.

1. Klicken Sie auf dem **Begrüßungsbildschirm** des EKM 3.0 Installationsassistenten auf **Weiter**.

   Das Fenster **Lizenzvereinbarung** wird angezeigt.
2. Wählen Sie die Optionsschaltfläche, um die Bedingungen der Lizenzvereinbarung anzunehmen.
3. Klicken Sie auf **Weiter**.

ANMERKUNG: Das EKM 3.0-Installationsprogramm führt Überprüfungen der Systemvoraussetzungen durch. Das Installationsprogramm überprüft, ob das System die Mindestanforderungen erfüllt und konfiguriert EKM 3.0 für Ihr System.

Beziehen Sie sich auf Überprüfungen der Systemvoraussetzungen.

Es wird der Bildschirm **Erneute Verwendung eines Installationsprofils** angezeigt.

4. *Wenn Sie EKM 3.0 zum ersten Mal installieren*, dann lassen Sie das Kontrollkästchen **Erneute Verwendung eines EKM 3.0-Installationsprofils** deaktiviert.

   Wenn Sie EKM 3.0 neu installieren, oder EKM 3.0 auf dem Sekundärserver installieren und ein Installationsprofil verwenden wollen, das Sie in einer vorherigen Installation gespeichert haben, dann führen Sie die folgenden Schritte durch:
   a) Aktivieren Sie das Kontrollkästchen **Erneute Verwendung eines EKM 3.0-Installationsprofils**. Die Auswahl des Kontrollkästchens aktiviert das Feld **Dateispeicherort**.
   b) Klicken Sie auf **Auswahl** und navigieren Sie zu dem Installationsprofil, das bei der vorherigen Konfiguration und Installation von EKM 3.0 erstellt wurde (z.B. **E:\EKM_config.txt** in Windows, oder **/tmp/ekm_config** in Linux).

      Sie können ein Wechsellaufwerk oder eine Netzwerkfreigabe verwenden, um das Installationsprofil aus dem Speicherort zu übertragen, in dem Sie es gespeichert haben.

ANMERKUNG: Das Installationsprofil füllt in der Installations-GUI alle Eingabefelder, mit Ausnahme der Kennwörter, mit den gleichen Angaben aus, die Sie in einer vorherigen Installation verwendet haben. Wenn Sie ein Installationsprofil verwenden, müssen Sie alle Kennwörter erneut eingeben.

ANMERKUNG: Wenn Sie EKM 3.0 auf einem Sekundärserver installieren, müssen Sie das Installationsprofil des primären EKM 3.0 Servers erneut verwenden, um sicherzustellen, dass die Eingabeparameter die gleichen sind.

5. Klicken Sie auf **Weiter**.

   Es wird der Bildschirm **Datenbank** angezeigt. Auf diesem Bildschirm erstellen Sie das EKM DB2 Datenbank-Administratorkonto.

ANMERKUNG: Dieser Bildschirm und die nächsten beiden Bildschirme erstellen jeweils ein unterschiedliches Konto. Notieren Sie sich alle Benutzernamen und Kennwörter, die Sie für diese Konten erstellen.

6. Das Feld **Datenbankspeicherort** weist als Standardeinstellung einen festen Speicherort auf. Dell empfiehlt, dass Sie den Standardspeicherort beibehalten. Dies ist der Speicherort, auf dem das Installationsprogramm die EKM 3.0 DB2 Software installiert.

7. Geben Sie im Feld **Datenbank-Benutzernamen** gemäß der folgenden Kriterien einen Benutzernamen ein:

   - Darf nur kleingeschriebene Buchstaben (a-z), Zahlen (0-9) und das Unterstreichungszeichen (_) enthalten.
   - Darf nicht länger als acht Zeichen sein
   - Darf nicht mit „ibm", „sys", „sql", oder einer Zahl beginnen
   - Darf nicht mit einem Unterstreichungszeichen beginnen oder enden
   - Darf kein DB2–reserviertes Wort (zum Beispiel: „users", „admins", „guests", „public" und „local") bzw. kein SQL-reserviertes Wort sein
   - Darf kein Benutzername eines im System vorhandenen Benutzers sein

   Dies ist die Kennung (ID) des EKM 3.0 DB2 Datenbank-Administratorkontos. EKM 3.0 erstellt ein lokales Benutzerkonto mit diesem Benutzernamen.

8. Geben Sie im Feld **Datenbankkennwort** ein Kennwort für das EKM DB2 Datenbank-Administratorkonto ein. Geben Sie im Feld **Datenbank-Kennwort bestätigen** das Kennwort erneut ein.

ANMERKUNG: Bei allen Kennwörtern wird zwischen Groß- und Kleinschreibung unterschieden.

ANMERKUNG: Dell empfiehlt die Verwendung sicherer Kennwörter für alle EKM 3.0-Benutzerkonten.

9. Geben Sie im Feld **Datenbankdatenlaufwerk** den Speicherort des Datenbank-Laufwerks an. Dies ist der Speicherort, in dem die EKM 3.0 DB2-Daten gespeichert werden. Geben Sie in Windows einen Laufwerksbuchstaben und einen Doppelpunkt (:) ein. Geben Sie in Linux einen Ordnerspeicherort ein, zum Beispiel **/home/ekmdb2**.

10. Geben Sie im Feld **Datenbankname** einen Namen für die EKM 3.0 DB2-Datenbank ein.

11. Die Standardeinstellung des Feldes **Datenbankport** ist **50010** in Windows und **50000** in Linux.

    Alle von EKM 3.0 verwendeten und während des EKM 3.0-Installationsvorgangs eingestellten Ports werden mit den empfohlenen Portadressen voreingestellt. Dell empfiehlt nachdrücklich, dass Sie diese empfohlenen Portadressen verwenden. Wenn Sie die Verwendung eines sekundären Servers planen und bei der Installation von EKM 3.0 eine Portadresse ändern, dann muss die Portadresse für die primären und sekundären EKM 3.0-Server gleich sein.

ANMERKUNG: Alle während des Installationsvorgangs verwendeten Ports müssen für das Installieren von EKM 3.0 offen sein. Überprüfen Sie folgendermaßen, ob sie offen sind:

So überprüfen Sie in Windows, ob die Ports offen sind:

a. Navigieren Sie zu: **<*Stammverzeichnis*>:\Windows\System32\drivers\etc**.
b. Öffnen Sie die Textdatei **Services**.

c. Überprüfen Sie die Datei und vergewissern Sie sich, dass die Portnummer vorhanden ist, die Sie im Feld **Datenbankport** verwenden wollen. Wenn der Port verfügbar ist, wird er nicht aufgeführt.

So überprüfen Sie in Linux, ob die Ports offen sind:

a. Öffnen Sie die Datei **/etc/services**.

b. Überprüfen Sie die Datei und vergewissern Sie sich, dass die Portnummer vorhanden ist, die Sie im Feld **Datenbankport** verwenden wollen. Wenn der Port verfügbar ist, wird er nicht aufgeführt.

12. Klicken Sie auf **Weiter**.

    Es wird der Bildschirm **EKM Administrator** angezeigt. Auf diesem Bildschirm erstellen Sie das EKM 3.0 Administrator (superuser)-Konto. Dieses Konto wird zur Erstellung neuer Benutzer und neuer Gruppen verwendet und für die Zuweisung derer Berechtigungen.

13. Geben Sie im Feld **Administratorbenutzername** einen EKM 3.0 Administratorbenutzernamen ein. (Dies kann jeder beliebige Name sein, mit Ausnahme von **tklmadmin**.)

14. Geben Sie im Feld K**ennwort** ein Kennwort für das EKM 3.0 Administratorkonto ein. Geben Sie im Feld **Kennwort bestätigen** das Kennwort erneut ein.

15. Klicken Sie auf **Weiter**.

    Es wird der Bildschirm **Encryption Manager** (Verschlüsselungsmanager) angezeigt. Auf diesem Bildschirm erstellen Sie das EKM 3.0 Encryption Manager (TKLMAdmin) Konto. Dies ist das reguläre Benutzerkonto. Es wird für die tägliche Schlüsselverwaltung verwendet. Das Feld **TKLMAdmin-Benutzername** ist bereits mit **tklmadmin** ausgefüllt. Dies ist der erforderliche EKM Encryption Manager-Name.

16. Geben Sie im Feld **TKLMAdmin-Kennwort** ein Kennwort für das EKM 3.0 Encryption Manager-Konto ein. Geben Sie im Feld **TKLMAdmin-Kennwort bestätigen** das Kennwort erneut ein.

17. Die Standardeinstellung des **EKM-Ports** ist in Windows und Linux **16310.** Dies ist der empfohlene Port. Klicken Sie auf **Weiter**.

ANMERKUNG: Wenn der bereitgestellte Port von einem anderen Dienst verwendet wird, dann fordert Sie das EKM 3.0-Installationsprogramm zur Auswahl eines anderen Ports aus. Verwenden Sie den **netstat-Befehl,** um zu bestimmen, ob die Ports gerade verwendet werden und wählen Sie anschließend einen verfügbaren Port aus. Notieren Sie die Portnummer. Sie werden diesen Port für den Zugriff auf das EKM 3.0-Portal verwenden.

Es wird der Bildschirm **Migration** angezeigt. Dieser Bildschirm wird für die Migration von EKM 2.X auf EKM 3.0 verwendet.

Wenn Sie eine EKM 2.X-Version haben, die Sie auf EKM 3.0 migrieren wollen, müssen Sie diese jetzt migrieren. Beziehen Sie sich auf Migration einer Encryption Key Manager (EKM) 2.X-Version während der EKM 3.0-Installation.

ANMERKUNG: Sie können nur EKM 2.X-Versionen migrieren, die zur Schlüsselerstellung verwendet wurden.

Wenn Sie keine EKM 2.X-Version für die Migration in EKM 3.0 haben, dann

a) Lassen Sie das Kontrollkästchen **Migration von EKM 2.X auf EKM 3.0** deaktiviert und klicken Sie auf **Weiter**.

   Es wird ein Popup-Bestätigungsfenster angezeigt.

b) Wenn Sie sich dafür entschieden haben, keine EKM 2.X-Version zu migrieren, dann klicken Sie im Popup-Fenster zur Bestätigung dessen, das Sie nicht auf eine EKM 2.0-Version migrieren auf **Ja** .

   Der Bildschirm **Konfigurations-Zusammenfassung** wird angezeigt.

18. Aktivieren Sie auf dem Bildschirm **Konfigurations-Zusammenfassung** das Kontrollkästchen **Profil speichern**.

    Das Feld **Dateiverzeichnis** wird aktiviert.

ANMERKUNG: Dell empfiehlt das Speichern des Installationsprofils für den Fall, dass EKM 3.0 in einer Notfallwiederherstellungssituation neu installiert werden muss. Für die Erstellung eines sekundären EKM 3.0-Server ist ein gespeichertes Installationsprofil erforderlich.

ANMERKUNG: Dell empfiehlt, dass Sie ein Wechsellaufwerk als den Speicherort verwenden. Wenn Sie ein Wechsellaufwerk verwenden, müssen Sie das Laufwerk einschieben, bevor Sie auf **Weiter** klicken. Das Wechsellaufwerk muss eingeschoben bleiben, bis die Installation abgeschlossen ist. Optional können Sie die Datei in einem Speicherort des lokalen Laufwerks speichern und die Datei später auf das Wechsellaufwerk kopieren.

ANMERKUNG: Der in dieses Feld eingegebene Pfad muss einen Dateinamen enthalten. Geben Sie nicht nur einen Ordnernamen ein. Der Dateipfad muss bis hin zum Ordnernamen vorhanden sein und der für das Installationsprofil verwendete Dateiname darf nicht vorhanden sein.

19. Geben Sie in das Feld **Dateiverzeichnis** den Speicherort und Dateinamen des Installationsprofils ein, das Sie erstellen, oder klicken Sie auf **Auswahl** und wählen Sie einen Speicherort aus und geben Sie anschließend einen Dateinamen ein.

    Dies ist der Speicherort, in dem Sie das zu speichernde Installationsprofil speichern wollen und der Name, unter dem Sie es speichern wollen.

    EKM 3.0 speichert das Installationsprofil bei Fertigstellung der EKM 3.0-Installation. Wenn Sie eine Primär/Sekundärserverkonfiguration verwenden, müssen Sie während der Installation des sekundären EKM 3.0 Servers das Installationsprofil des primären EKM 3.0-Servers verwenden, um die Installationseingabefelder automatisch auszufüllen.

    Optional können Sie, wenn Sie auf dem gleichen Server neu installieren und die gleichen Felder verwenden wollen, dieses Installationsprofil verwenden, um die Installationseingabefelder automatisch auszufüllen.

ANMERKUNG: Dell empfiehlt, dass Sie zur späteren Bezugnahm den Bildschirm **Konfigurations-Zusammenfassung** erfassen oder ausdrucken.

20. Klicken Sie auf dem Bildschirm **Konfigurations-Zusammenfassung** auf **Weiter**.

    Der Bildschirm **Installations-Zusammenfassung** wird angezeigt.

21. Überprüfen Sie die Informationen auf dem Bildschirm **Konfigurations-Zusammenfassung**.
22. Klicken Sie auf **Installieren**.

ANMERKUNG: Das Software-Installationsverfahren nimmt etwa 45 Minuten in Anspruch. Schalten Sie das System nicht aus, bevor die Installation abgeschlossen wurde.

ANMERKUNG: Wenn Sie vorhaben einen sekundären EKM 3.0-Server einzurichten, dann installieren Sie EKM 3.0 so lange nicht auf dem sekundären Server, bis die Installation des primären EKM 3.0 Servers abgeschlossen wurde.

23. Wenn die Installation abgeschlossen wurde, klicken Sie auf **Fertig**.

ANMERKUNG: Wenn Sie eine EKM 2.X-Version auf das neu installierte EKM 3.0 migriert haben, dann empfiehlt Dell nachdrücklich, dass Sie eine Sicherung von EKM 3.0 erstellen, um sicherzustellen, dass die neuen Schlüssel nicht verloren gehen. Beziehen Sie sich auf Erstellung einer Sicherung des Keystores.

ANMERKUNG: Wenn Sie EKM 3.0 neu installieren und die Installation schlägt aufgrund einer unvollständigen Deinstallation fehl, dann führen Sie die Deinstallation manuell durch. Beziehen Sie sich auf Manuelle Deinstallation von EKM 3.0 in Windows.

3

Einrichtung von primären und sekundären EKM 3.0-Servern

Dieses Kaptel beschreibt das Installieren, Verwenden und Deinstallieren von EKM 3.0 auf den primären und sekundären Servern.

VORSICHT: Um möglichen Datenverlust aufgrund eines EKM 3.0-Serverausfalls zu vermeiden, empfiehlt Dell die Verwendung eines Primär/Sekundärserver-Setups. Diese Konfiguration stellt Redundanz für den Fall bereit, dass der primäre EKM 3.0-Server ausgefallen oder nicht verfügbar ist.

ANMERKUNG: Es ist nicht möglich, einen primären EKM 3.0 und einen sekundären EKM 2.X Server zu haben, oder umgekehrt.

Installation von EKM 3.0 auf dem primären Server

Während der Installation von EKM 3.0 auf dem primären Server müssen Sie die Option zum Speichern des Instalationsprofils auswählen. Kopieren Sie das gespeicherte Installationsprofil auf ein Wechsellaufwerk oder eine Serverfreigabe, wenn die Installation von EKM 3.0 auf dem primären Server abgeschlossen wurde. Beziehen Sie sich auf Installation von EKM 3.0.

Verwendung von EKM 3.0 auf dem primären Server

Auf dem primärenEKM 3.0 Server führen Sie alle Aufgaben für die Verwaltung von Verschlüsselungscodes durch. Standardmäßig ist der primäre EKM 3.0 Server auf **Automatische Annahme aller neuen Geräte-Kommunikationsanfragen** eingestellt. Beziehen Sie sich auf Konfigurieren von EKM 3.0 zum Akzeptieren von Geräten, die EKM 3.0 kontaktieren, um Schlüssel zu erhalten, um Einzelheiten über das Anzeigen und Konfigurieren dieser Einstellung zu erhalten. Beziehen Sie sich auf Durchführen von Sicherungen und Wiederherstellen aus einer Sicherung.

Falls der primäre EKM 3.0 Server aus irgendeinem Grund ersetzt werden muss, installieren Sie EKM 3.0 auf einem neuen physikalischen Server, indem Sie das Installationsprofil aus der ursprünglichen primären EKM 3.0-Installation verwenden. Stellen Sie den neuen primären EKM 3.0 Server mit der aktuellsten Sicherung wieder her und aktualisieren Sie anschließend alle Geräte, sodass diese für Schlüsselanforderungen mit dem neuen primären EKM 3.0 Server kommunizieren. Beziehen Sie sich auf das Benutzerhandbuch Ihrer Band-Library, um Einzelheiten über das Ändern der IP-Adresse des für Schlüsselanforderungen verwendeten EKM 3.0 Servers zu erfahren. Lesen Sie den Abschnitt „Dokumentation und Referenzmaterialien“ der Datei **ReadThisFirst.txt** auf dem EKM 3.0 Installationsdatenträger, um das Benutzerhandbuch der Band-Library ausfindig zu machen.

Installation von EKM 3.0 auf dem sekundären Server

ANMERKUNG: Installieren Sie EKM 3.0 so lange nicht auf dem sekundären Server, bis die Installation von EKM 3.0 auf dem primären Server abgeschlossen wurde.

Das System, auf dem EKM 3.0 als sekundärer Server installiert ist, muss die gleiche Version des Betriebssystems haben, wie die, die auf dem primären EKM 3.0 Server installiert ist. EKM 3.0 unterstützt das Mischen von Betriebssystemen zwischen primären und sekundären Servern nicht.

Installieren Sie EKKM 3.0 auf dem sekundären Server, indem Sie die Verfahren in EKM 3.0-Installation verwenden. Verwenden Sie das Installationsprofil, das Sie bei der Installation von EKM auf dem primären Server gespeichert haben. Sie müssen manuell die gleichen Kennwörter eingeben, die Sie bei der Installation von EKM 3.0 auf dem primären Server verwendet haben.

Verwendung von EKM 3.0 auf dem sekundären Server

Der sekundäre EKM 3.0 Server wird verwendet, um im Falle eines inaktiven oder nicht erreichbaren primären Servers Redundaz bereitzustellen.

Verwenden Sie die auf dem primären EKM 3.0 Server erstellte Sicherung, um den Wiederherstellungsvorgang auf dem sekundären EKM 3.0 Server in regelmäßigen Abständen durchzuführen und die primären und sekundären Server synchronisiert zu halten. Beziehen Sie sich auf Durchführen von Sicherungen und Wiederherstellen aus einer Sicherung.

Standardmäßig ist der sekundäre EKM 3.0 Server ebenfalls auf **Automatische Annahme aller neuen Geräte-Kommunikationsanfragen** eingestellt. Dell empfiehlt, die Einstellung nach jeder Wiederherstellung auf **Nur manuell hinzugefügte Geräte für die Kommunikation akzeptieren** zu ändern. Dadurch wird verhindert, dass der sekundäre EKM 3.0 Server Schlüssel an neue Geräte vergibt, die nicht zum primären EKM 3.0 Server hinzugefügt werden. Beziehen Sie sich auf Konfigurieren von EKM 3.0 zum Akzeptieren von Geräten, die EKM 3.0 kontaktieren, um Schlüssel zu erhalten, um Einzelheiten über das Anzeigen und Konfigurieren dieser Einstellung zu erhalten.

Wenn der primäre 3.0 Server vorübergehend inaktiv oder nicht verfügbar ist, müssen Sie die Wiederherstellung auf dem sekundären Server unter Verwendung der letzten Sicherung durchführen, die auf dem primären EKM 3.0 Server erstellt wurde.

ANMERKUNG: Wenn der primäre 3.0 Server inaktiv oder nicht verfügbar ist und der sekundäre EKM 3.0 Server für die Unterstützung von Schlüsselanforderungen durch Geräte verwendet wird, empfiehlt Dell, dass Sie keinerlei Verwaltungs- und operationale Aufgaben auf dem sekundären EKM 3.0 Server durchführen.

Deinstallation von EKM 3.0 von den primären und sekundären Servern

Beziehen Sie sich für das Verfahren zur Deinstallation von EKM 3.0 von den primären und sekundären Servern auf Deinstallation von EKM 3.0.

4

Durchführung von Sicherungen und Wiederherstellung aus einer Sicherung

Sie können jederzeit Sicherungen durchführen. Das Durchführen einer Sicherung erstellt eine Sicherungsdatei, die den Keystore enthält, der Geräte und Schlüssel enthält.

Sicherungen enthalten keine Gerätegruppen, Benutzer, oder Benutzergruppen. Diese sind in der DB2-Datenbank enthalten.

Sie können jederzeit aus einer Sicherung wiederherstellen.

ANMERKUNG: Wenn Schlüssel nicht gesichert werden, werden sie nicht vergeben. Wenn Schlüssel nicht für die Vergabe verfügbar sind, schlagen verschlüsselte Sicherungsaufträge fehl.

Erstellung einer Sicherung des Keystores

Dieses Kapitel beschreibt das Sichern des Keystores.

1. Melden Sie sich am EKM 3.0 Portal an. Beziehen Sie sich auf Anmeldung am Encryption Key Manager 3.0 Portal.

   Es wird der Bildschirm **Willkommen bei Dell Encryption Key Manager** angezeigt.
2. Navigieren Sie im Navigationsfensterbereich zu **Dell Encryption Key Manager → Sicherung oder Wiederherstellung** .

   Es wird der Bildschirm **Sicherung oder Wiederherstellung** angezeigt.
3. Klicken Sie neben dem Feld **Sicherung des Repository-Speicherortes** auf **Durchsuchen** und navigieren Sie zu dem Ordner, in dem Sie die Sicherungsdatei speichern wollen (zum Beispiel **C:\EKM_Backup** in Windows, oder **/Stammverzeichnis/EKM_Backup** in Linux.

ANMERKUNG: Der Ordner muss vor dem Starten der Sicherung vorhanden sein, anderenfalls schlägt die Sicherung fehl. Wenn Sie einen neuen Ordner verwenden wollen, dann erstellen Sie diesen, bevor Sie einen Versuch zum Erstellen einer Sicherung unternehmen.

4. Klicken Sie im Popup-Fenster **Verzeichnis durchsuchen** auf **Auswahl**, um zurück zum Bildschirm **Sicherung oder Wiederherstellung** zu gelangen.
5. Klicken Sie auf **Sicherung erstellen**.

   Das Fenster **Sicherung erstellen** wird angezeigt.
6. Erstellen Sie im Feld **Kennwort erstellen** ein Kennwort für die Sicherung. Das Kennwort darf nicht weniger als sechs Zeichen haben.

ANMERKUNG: Dell empfiehlt die Verwendung von sicheren Kennwörtern für alle EKM 3.0-bezogenen Aktivitäten .

7. Geben Sie im Feld **Kennwort-Neueingabe** das Kennwort erneut ein.
8. (Optional) Geben Sie im Feld **Sicherungsbeschreibung** eine Beschreibung für die Sicherungsdatei ein. Wenn Sie keine Beschreibung eingeben, wird eine Standardbeschreibung zur Sicherungsdatei hinzugefügt.

ANMERKUNG: In einigen Browserversionen kann das standardmäßige Feld für die Beschreibung nicht geändert werden. Beziehen Sie sich für weitere Informationen auf Bekannte Probleme und Lösungen.

9. Klicken Sie auf **Sicherung erstellen**.

   Es wird ein Popup-Bestätigungsfenster angezeigt.

10. Klicken Sie im Popup-Bestätigungsfenster auf **OK**. Der Sicherungsvorgang wird ausgeführt.

ANMERKUNG: Verwenden Sie das System nicht während der Ausführung eines Sicherungsvorgangs. Klicken Sie auf die Aktualisierungsschaltfläche Ihres Browsers, wenn die Inhalte von EKM 3.0 für längere Zeit grau unterlegt sind.

11. Wenn die Sicherungsdatei erstellt wurde, wird ein Popupfenster mit **Informationen** angezeigt, das die erfolgreiche Erstelllung der Datei bestätigt. Klicken Sie im Popup-Fenster auf **OK**. Die erstellte Sicherungsdatei wird in der Tabelle auf dem Bildschirm **Sicherung und Wiederherstellung** angezeigt.
12. Klicken Sie am unteren Bildschirmrand auf **Zurück auf die Startseite**.

    Es wird der Bildschirm **Willkommen bei Dell Encryption Key Manager** angezeigt.

Wiederherstellung aus einer Sicherung

Sie können aus einer Sicherung wiederherstellen. Sie können eine Sicherung zur Erstellung sekundärer Server, wie auch zur Neuerstellung des EKM 3.0 Servers in einer Notfallwiederherstellungssituation verwenden.

VORSICHT: Führen Sie Wiederherstellungen nur mittels Sicherungen durch, die auf dem gleichen System oder einem anderen EKM 3.0 Server erstellt wurden. Sie können nicht aus einer Sicherung wiederherstellen, die auf einem anderen System unter Verwendung unterschiedlicher Installationseigenschaften erstellt wurde.

1. Melden Sie sich am EKM 3.0 Portal an. Beziehen Sie sich auf Anmeldung am Encryption Key Manager 3.0 Portal.

   Es wird der Bildschirm **Willkommen bei Dell Encryption Key Manager** angezeigt.
2. Navigieren Sie im Navigationsfensterbereich zu **Dell Encryption Key Manager → Sicherung oder Wiederherstellung** .

   Es wird der Bildschirm **Sicherung oder Wiederherstellung** angezeigt.
3. Wählen Sie die Sicherung aus, aus der Sie wiederherstellen wollen.
4. Klicken Sie oben in der Tabelle auf **Aus Sicherung wiederherstellen**.

   Es wird das Unterfenster **Aus Sicherung wiederherstellen** angezeigt.
5. Geben Sie das Kennwort für die Sicherungsdatei ein.
6. Klicken Sie auf **Sicherung wiederherstellen**.

   Es wird ein Popup-Bestätigungsfenster angezeigt.

VORSICHT: Alle Schlüssel, die Sie nach der Sicherung erstellt haben, gehen zusammen mit dem Zugriff auf alle mit Schlüsseln verschlüsselten Daten verloren. Es gibt keine Möglichkeit, verloren gegangene Schlüssel wiederherzustellen.

7. Klicken Sie im Popup-Bestätigungsfenster auf **OK**.
8. Nach der Wiederherstellung aus der Sicherung heraus müssen Sie den EKM 3.0 Server manuell stoppen und starten. Beziehen Sie sich auf Starten und Stoppen des EKM 3.0 Servers in Windows oder Starten und Stoppen des EKM 3.0 Servers in Linux.

5

EKM 3.0 - Verwendung

Dieses Kapitel beschreibt einige grundlegende EKM 3.0-Vorgänge.

ANMERKUNG: EKM 3.0 basiert auf IBM Tivoli Key Lifecycle Manager (TKLM) V2 FixPack 2, wurde jedoch durch Auswahl des entsprechenden Subsets der TKLM-Band-Funktionen für die Unterstützung von Dell Band-Library-Umgebungen angepasst.

Informationen zur Verwendung von EKM 3.0 sind in dieser Anleitung nicht enthalten, beziehen Sie sich hierfür auf die TKLM-Dokumentation, in der die folgenden Themen enthalten sind:

- IBM Tivoli Key Manager 2.0 *Schnellstart-Handbuch*
- IBM Tivoli Key Manager 2.0 *Installations- und Konfigurationshandbuch*
- IBM Tivoli Key Manager 2.0 *Produktübersicht/Szenariohandbuch*

Lesen Sie für Informationen zum Zugriff auf die TKLM-Dokumentation den Abschnitt „Dokumentation und Referenzmaterialien“ der Datei **ReadThisFirst.txt** auf dem EKM 3.0 Installationsdatenträger.

Einige in der IBM TKLM-Dokumentation beschriebenen Bildschirme und Funktionalitäten sind in Dell EKM 3.0 nicht aktiviert. EKM 3.0 enthält nur eine Untermenge an Funktionen, die zur Unterstützung von Dell PowerVault Band-Libraries benötigt werden.

Anmeldung am Encryption Key Manager 3.0 Portal

Führen Sie die folgenden Schritte durch, um sich am Encryption Key Manager 3.0 Portal anzumelden:

1. Öffnen Sie einen Browser und geben Sie die folgende URL ein, um das EKM 3.0 Portal zu öffnen:
   http://*<EKM 3.0_Server_IP_Adresse>*:*<EKM_3.0_Port_Nummer>*

   ANMERKUNG: Die angegebene Portnummer ist die, die Sie während der EKM 3.0 Installation zur Verfügung gestellt haben. Die Standardeinstellung ist **16310**.

   Wenn Sie die Portnummer nicht kennen, dann beziehen Sie sich auf folgende Vorgehensweise:

   In Windows Beziehen Sie sich auf den Wert der **WC_defaulthost**-Eigenschaft in der folgenden Datei: ***<Stammverzeichnis>*:\Dell\EKM\profiles\TIPProfile\properties\portdef.props**.

   In Linux Beziehen Sie sich auf den Wert der **WC_defaulthost**-Eigenschaft in der folgenden Datei: **/opt/dell/ekm/profiles/TIPProfile/properties/portdef.props**.

   ANMERKUNG: Wenn eine Fehlermeldung angezeigt wird, die besagt, dass die Seite nicht gefunden werden kann, wird der EKM 3.0-Dienst möglicherweise nicht ausgeführt. Beziehen Sie sich auf Starten und Stoppen des EKM 3.0 Servers in Windows oder Starten und Stoppen des EKM 3.0 Server in Linux.

   Es wird das EKM 3.0 Anmeldefenster angezeigt.
2. Melden Sie sich an EKM 3.0 unter Verwendung des EKM 3.0 Encryption Manager-Benutzernamens (**tklmadmin**) und des Kennwortes an, das während der EKM 3.0 Installation bereitgestellt wurde.

   Es wird der Bildschirm **Willkommen bei Dell Encryption Key Manager** angezeigt.

Erstellung eines Master-Keystores

Dieses Kapitel beschreibt die Erstellung des Master-Keystores. Sie müssen den Master-Keystore bei der Erstanmeldung an EKM 3.0 erstellen.

ANMERKUNG: Wenn Sie während der EKM 3.0-Installation einen EKM 2.X-Keystore migriert haben, wurde bereits ein Keystore erstellt und dieses Verfahren ist nicht anwendbar.

ANMERKUNG: Beziehen Sie sich später, wenn Sie weitere Schlüssel und/oder Schlüsselgruppen erstellen wollen, auf Erstellung von Schlüsselgruppen für die Gerätegruppe.

Führen Sie die folgenden Schritte durch, um den Master-Keystore zu erstellen.

1. Klicken Sie im Bildschirm **Willkommen bei Dell Encryption Key Manager** auf **Zur Erstellung des Master-Keystores hier klicken**.

   Es wird der **Keystore**-Bildschirm angezeigt.
2. Behalten Sie die Standardwerte für **Keystore-Typ**, **Keystore-Pfad** und **Keystore-Namen** bei.

   Die Standardwerte sind: **Keystore-Typ**: JCEKS und **Keystore-Name**: defaultKeyStore. Der Standardwert für den **Keystore-Pfad** in Windows ist: **<*Stammverzeichnis*>:\Dell\EKM\products\tklm\keystore**. Der Standardwert für den **Keystore -Pfad** in Linux ist: **/opt/dell/ekm/products/tklm/keystore**.
3. Erstellen Sie im **Kennwort**-Feld ein Kennwort für den Standard-Keystore. Dieses Kennwort darf nicht weniger als sechs Zeichen haben.
4. Geben Sie im Feld **Kennwort-Neueingabe** das Kennwort erneut ein.
5. Klicken Sie auf **OK**.

   Der Bildschirm **Keystore** bestätigt die erfolgreiche Erstellung des Keystores.
6. Erstellen Sie eine Sicherung des Keystores. Beziehen Sie sich auf Durchführen von Sicherungen und Wiederherstellen aus einer Sicherung.

Aktivieren der Firewall in EKM 3.0 Server

ANMERKUNG: Beziehen Sie sich auf die Dokumentation Ihres Betriebssystems, um Anweisungen zum Konfigurieren der Firewall zu erhalten.

EKM 3.0 kommuniziert über das Netzwerk mit der Band-Library. Wenn die Firewall auf dem System aktiviert ist, auf dem EKM 3.0 installiert ist und die erforderlichen Ports nicht geöffnet wurden, schlägt die Kommunikation zwischen EKM 3.0 und der Band-Library fehl. Wenn Sie die Firewall auf dem System aktivieren müssen, auf dem EKM 3.0 installiert ist, dann führen Sie die folgenden Schritte zum Aktivieren der Kommunikation zwischen EKM 3.0 und der Band-Library durch:

ANMERKUNG: Dies sind die von EKM 3.0 verwendeten Standardports. Wenn Ihre Band-Library für die Verwendung anderer Ports konfiguriert wurde, dann stellen Sie sicher, dass Sie diese Portnummern in den Firewalleinstellungen und in der EKM 3.0-Konfiguration verwenden.

ANMERKUNG: Wenn Sie für EKM 3.0 eine Primär-/Sekundärseverkonfiguration verwenden, dann wiederholen Sie dieses Verfahren für den sekundären Server.

1. Öffnen Sie die folgenden Ports für die entsprechenden Protokolle:
   - TCP: 3801
   - SSL: 443
2. Wenn Ihre Firewall so konfiguriert wurde, dass sie nur bestimmte IP-Adressen und/oder Subnetzmasken für die Kommunikation mit den obigen Ports zulässt, dann stellen Sie sicher, dass die IP-Adresse und/oder Subnetzmaske in der Liste der zulässigen IP-Adressen und/oder Subnetzmasken enthalten ist.

Um auf die Band-Library-Netzwerkkonfiguration zuzugreifen, melden Sie sich an der RMU (Remote Management Unit) der Band-Library an und machen Sie die Netzwerkeinstellungen ausfindig. Beziehen Sie sich für weitere Informationen auf das Benutzerhandbuch der Band-Library. Lesen Sie den Abschnitt „Dokumentation und Referenzmaterialien“ der Datei **ReadThisFirst.txt** auf dem EKM 3.0 Installationsdatenträger.

3. Wenn Sie die Porteinstellungen für die Kommunikation zwischen EKM 3.0 und der Band-Library zu einem späteren Zeitpunkt ändern wollen, dann stellen Sie sicher, dass die Ports in den Einstellungen der Band-Library, EKM 3.0, und der Firewall des Systems, auf dem EKM 3.0 installiert ist geändert werden.

Konfigurieren von EKM 3.0 zum Akzeptieren von Geräten, die EKM 3.0 kontaktieren, um Schlüssel zu erhalten

Dieses Kapitel beschreibt, wie das Verhalten von EKM 3.0 konfiguriert wird, um mit Geräten umzugehen, die versuchen, sich mit EKM 3.0 zum Abruf von Schlüsseln zu verbinden. Beziehen Sie sich auf das Benutzerhandbuch Ihres Gerätes, um Einzelheiten über das Vorgehen beim Verbinden mit EKM 3.0 für Schlüsselanfragen zu erfahren.

1. Melden Sie sich am EKM 3.0 Portal an. Beziehen Sie sich auf Anmeldung am Encryption Key Manager 3.0 Portal.
   Es wird der Bildschirm **Willkommen bei Dell Encryption Key Manager** angezeigt.
2. Navigieren Sie im Navigationsfensterbereich zu **Dell Encryption Key Manager → Schlüssel- und Geräteverwaltung**
   Es wird der Bildschirm **Schlüssel- und Geräteverwaltung** angezeigt.
3. Wählen Sie im Dropdown-Menü **Schlüssel und Geräte verwalten LTO** aus und klicken Sie auf **Start**.

ANMERKUNG: Beziehen Sie sich auf die TKLM-Dokumentation, um weitere Einzelheiten zu diesen Einstellungen zu erhalten. Lesen Sie für Informationen darüber, wie auf die TKLM-Dokumentation zugegriffen werden kann, den Abschnitt „Dokumentation und Referenzmatierialien“ der Datei **ReadThisFirst.txt** auf dem EKM 3.0 Installationsdatenträger.

4. Wählen Sie im Dropdown-Menü unten in der Tabelle einen der folgenden Vorgänge aus:

Automatische Annahme aller neuen Geräte-Kommunikationsanfragen	Schlüssel werden automatisch an neue Geräte vergeben. Dies ist die Standardeinstellung für EKM 3.0. Dell empfiehlt, dass Sie diese Einstellung für den primären EKM 3.0 Server beibehalten, jedoch nicht für den sekundären, falls Sie einen konfiguriert haben.
Nur manuell hinzugefügte Geräte für die Kommunikation akzeptieren	Schlüssel werden nur dann an Geräte vergeben, wenn die Geräte manuell hinzugefügt werden. Wenn Sie den sekundären EKM 3.0 Server konfigurieren, empfiehlt Dell, dass Sie diese Einstellung verwenden, sodass der sekundäre EKM 3.0 Server nicht automatisch Schlüssel an neue Geräte vergibt.
Neue Geräteanfragen mit ausstehender Zustimmung in Warteliste	Geräte, die EKM 3.0 kontaktieren, werden einer Warteliste hinzugefügt.

Erstellen einer Gerätegruppe

Dieses Verfahren erstellt eine Gerätegruppe. Wenn Sie eine Standard-Gerätegruppe verwenden, dann überspringen Sie diesen Abschnitt.

Gerätegruppen werden zur Verwaltung von Schlüsseln verwendet, die an eines oder mehrere Geräte vergeben werden. Dell empfiehlt, dass Sie Gerätegruppen verwenden, um ein Subset (Untermenge) Ihrer Geräte basierend auf den Anforderungen Ihrer Organisation zu verwalten.

Führen Sie die folgenden Schritte durch, um eine neue Gerätegruppe zu erstellen:

1. Melden Sie sich am EKM 3.0 Portal an. Beziehen Sie sich auf Anmeldung am Encryption Key Manager 3.0 Portal.

Es wird der Bildschirm **Willkommen bei Dell Encryption Key Manager** angezeigt.

2. Navigieren Sie im Navigationsfensterbereich zu **Dell Encryption Key Manager** → **Erweiterte Konfiguration** → **Gerätegruppe**.

   Es wird der Bildschirm **Gerätegruppen verwalten** angezeigt.

3. Klicken Sie oben in der Tabelle auf **Erstellen**.

   Es wird das Unterfenster **Gerätegruppe erstellen** angezeigt.

4. Wählen Sie unter **Gerätefamilie** die Optionsschaltfläche **LTO** aus.

5. Geben Sie im Feld **Gerätegruppenname** einen Gerätegruppennamen ein. Dell empfiehlt, dass Sie einen Namen eingeben, der die Verwendung dieser Gerätegruppe widerspiegelt, beispielsweise **Buchhaltung**.

6. Klicken Sie auf **Erstellen**.

   Ein **Informationen** Popup-Fenster informiert Sie über die Gerätefamilieneinstellung.

7. Klicken Sie im **Informationen** Popup-Fenster auf **OK**.

   Die Gerätegruppe wird erstellt. Die neue Gerätegruppe wird in der Liste des Bildschirms **Gerätegruppen verwalten** angezeigt.

Erstellung von Schlüsselgruppen für eine Gerätegruppe

Schlüsselgruppen sind Gruppen von Schlüsseln für ein spezifisches Gerät. Dieses Kapitel beschreibt die Erstellung und Konfiguration von Schlüsselgruppen für ein bestimmtes Gerät. Für ein Gerät erstellte Schlüsselgruppen können mit keinem anderen Gerät verwendet werden.

Führen Sie für die Erstellung von Schlüsselgruppen für die Gerätegruppe die folgenden Schritte durch:

1. Melden Sie sich am EKM 3.0 Portal an. Beziehen Sie sich auf Anmeldung am Encryption Key Manager 3.0 Portal.

   Es wird der Bildschirm **Willkommen bei Dell Encryption Key Manager** angezeigt.

2. Navigieren Sie im Navigationsfensterbereich zu **Dell Encryption Key Manager** → **Schlüssel- und Geräteverwaltung**.

   Es wird der Bildschirm **Schlüssel- und Geräteverwaltung** angezeigt.

3. Wählen Sie im Dropdown-Menü **Schlüssel und Geräte verwalten** den Gerätegruppennamen aus, zu dem Sie die Schlüsselgruppe hinzufügen wollen.

4. Klicken Sie neben **Schlüssel- und Geräteverwaltung** auf **Start**.

   Im **Schlüssel- und Geräteverwaltung**-Dienstprogramm wird eine Seite für die von Ihnen gewählte Gerätegruppe angezeigt. Diese Seite führt alle Schlüsselgruppen und Geräte auf, die zu dieser Gerätegruppe gehören.

5. Klicken Sie in der Tabelle auf **Hinzufügen** und wählen Sie anschließend **Schlüsselgruppe** aus.

   Es wird das Unterfenster **Schlüsselgruppe erstellen** angezeigt.

6. Geben Sie im Feld **Schlüsselgruppenname** den Namen der Schlüsselgruppe ein.

7. Geben Sie im Feld **Anzahl der zu erstellenden Schlüssel** die Anzahl der zu erstellenden Schlüssel ein.

8. Geben Sie im Feld **Erste drei Buchstaben des Schlüsselnamens** ein beliebiges Präfix für den Schlüsselnamen ein.

9. Wenn Sie wollen, dass diese Schlüsselgruppe die Standardschlüsselgruppe ist, dann aktivieren Sie das Kontrollkästchen **Zur Standardschlüsselgruppe** machen.

10. Klicken Sie auf **Schlüsselgruppe erstellen**.

    Es wird ein Popup-Fenster mit einer **Warnung** angezeigt.

11. Wenn Sie eine Sicherung erstellen wollen, dann klicken Sie im Popup-Fenster mit der **Warnung** auf den blauen Link, um zum Bildschirm **Sichern und Wiederherstellen** geleitet zu werden. Beziehen Sie sich auf Durchführen von Sicherungen und Wiederherstellen aus einer Sicherung. Kehren Sie nach der Erstellung der Sicherung zum Bildschirm **Schlüssel- und Geräteverwaltung** zurück. Fahren Sie mit dem nächsten Schritt fort, wenn Sie zu diesem Zeitpunkt keine Sicherung erstellen wollen.

ANMERKUNG: Dell empfiehlt das Erstellen einer Sicherung, wenn Sie Änderungen an Schlüsseln, Schlüsselgruppen oder Gerätegruppen vornehmen.

12. Klicken Sie im Popup-Fenster mit der **Warnung** auf **OK**.

    Die Schlüsselgruppe wird erstellt. Der Bildschirm **Schlüssel- und Geräteverwaltung** zeigt die Schlüsselgruppen an.

13. Dieser Schritt ist optional. Überprüfen Sie, dass die Schlüssel erstellt wurden, indem Sie auf dem Bildschirm **Schlüssel- und Geräteverwaltung** die folgenden Schritte durchführen:
    a) Wählen Sie im Dropdown-Menü oben in der Tabelle **Schlüssel, Schlüsselgruppenmitgliedschaft und Laufwerke aus**.

       Die Schlüssel werden in der Tabelle angezeigt.
    b) Scrollen Sie nach unten, um die neuen Schlüssel ausfindig zu machen.

Hinzufügen eines Gerätes zu einer Gerätegruppe

Dieses Kapitel beschreibt das Hinzufügen eines Gerätes zu einer vorhandenen Gerätegruppe.

ANMERKUNG: Die Standard-Gerätegruppen in EKM 3.0 sind **FUTURE_DEVICES** und **LTO**.

ANMERKUNG: Um ein Gerät automatisch zu einer Gerätegruppe hinzuzufügen, müssen Sie eine Schlüsselgruppe und eine Sicherung erstellen, oder die Schlüsselpfad-Diagnose der Band-Library schlägt fehl und das Gerät wird nicht hinzugefügt. Beziehen Sie sich auf Erstellung von Schlüsselgruppen für eine Gerätegruppe und Erstellung einer Sicherung des Keystores, um weitere Informationen zu erhalten.

1. Melden Sie sich am EKM 3.0 Portal an. Beziehen Sie sich auf Anmeldung am Encryption Key Manager 3.0 Portal.

   Es wird der Bildschirm **Willkommen bei Dell Encryption Key Manager** angezeigt.
2. Wählen Sie im Dropdown-Menü **Schlüssel und Geräte verwalten** unter **Schlüssel- und Geräteverwaltung** die Gerätegruppe aus, die Sie verwenden wollen.
3. Klicken Sie auf **Start**.

   Im **Schlüssel- und Geräteverwaltung**-Dienstprogramm wird eine Seite für die von Ihnen gewählte Gerätegruppe angezeigt. Diese Seite führt alle Schlüsselgruppen und Geräte auf, die zu dieser Gerätegruppe gehören.
4. Wählen Sie aus dem Dropdown-Menü unten auf der Seite **Automatische Annahme aller neuen Geräte-Kommunikationsanfragen** aus.
5. Konfigurieren Sie die Band-Library für die Verbindung mit dem EKM 3.0 Server.

   Beziehen Sie sich für weitere Informationen auf das Benutzerhandbuch der Band-Library. Lesen Sie den Abschnitt „Dokumentation und Referenzmaterialien“ der Datei **ReadThisFirst.txt** auf dem EKM 3.0 Installationsdatenträger, um das Benutzerhandbuch der Band-Library ausfindig zu machen.
6. Führen Sie Schlüsselpfaddiagnosen in der RMU (Remote Management Unit) der Band-Library aus. Beziehen Sie sich für weitere Informationen auf das Benutzerhandbuch der Band-Library.

   Das neue Gerät wird auf dem Bildschirm **Schlüssel- und Geräteverwaltung** angezeigt.

ANMERKUNG: Wenn Sie ein Gerät manuell hinzufügen wollen, dann beziehen Sie sich auf die TKLM-Dokumentation. Beziehen Sie sich für Informationen über den Zugang zur TKLM-Dokumentation auf den Abschnitt „Dokumentation und Referenzmaterialien“ der Datei **ReadThisFirst.txt** auf dem EKM 3.0-Installationsdatenträger.

Hinzufügen und Löschen von Schlüsseln aus Schlüsselgruppen

Dieses Kapitel beschreibt, wie Sie Schlüssel zu Schlüsselgruppen hinzufügen und aus Schlüsselgruppen löschen.

ANMERKUNG: Das Löschen eines Schlüssels aus einer Schlüsselgruppe löscht den Schlüssel nicht; es entfernt den Schlüssel lediglich aus der Schlüsselgruppe. Wenn Sie einen einzelnen Schlüssel löschen wollen, dann beziehen Sie sich auf Löschen eines bestimmten Schlüssels.

ANMERKUNG: Beziehen Sie sich für Anweisungen zum Zugriff auf den Bildschirm **Schlüssel- und Geräteverwaltung** auf Erstellen von Schlüsselgruppen für die Gerätegruppe.

1. Melden Sie sich am EKM 3.0 Portal an. Beziehen Sie sich auf Anmeldung am Encryption Key Manager 3.0 Portal.
   Es wird der Bildschirm **Willkommen bei Dell Encryption Key Manager** angezeigt.
2. Navigieren Sie im Navigationsfensterbereich zu **Dell Encryption Key Manager → Schlüssel- und Geräteverwaltung**.
   Es wird der Bildschirm **Schlüssel- und Geräteverwaltung** angezeigt.
3. Wählen Sie im Dropdown-Menü **Schlüssel und Geräte verwalten** den Gerätegruppennamen aus, zu dem Sie die Schlüsselgruppe hinzufügen wollen.
4. Gehen Sie als Nächstes zu **Schlüssel- und Geräteverwaltung** und klicken Sie auf **Start**.
   Im Dienstprogramm **Schlüssel- und Geräteverwaltung** wird eine Seite für die Gerätegruppe angezeigt. Diese Seite führt alle Schlüsselgruppen und Geräte auf, die zu dieser Gerätegruppe gehören.
5. Wählen Sie die zu ändernde Schlüsselgruppe aus.
6. Klicken Sie oben in der Tabelle auf **Ändern**.
   Es wird das Unterfenster **Schlüsselgruppe ändern** angezeigt.
7. Wählen Sie im Unterfenster **Schlüsselgruppe ändern** die gewünschte Optionsschaltfläche.
   Wenn Sie die Optionsschaltfläche **Weitere Schlüssel in Schlüsselgruppe erstellen** auswählen, dann geben Sie im Feld **Anzahl der zu erstellenden Schlüssel** die Anzahl der Schlüssel ein. Geben Sie im Feld **Drei Anfangsbuchstaben des Schlüsselnamens** drei Buchstaben ein, die das Präfix der neuen Schlüssel werden.
   Wenn Sie das Feld **Schlüssel aus Schlüsselgruppe löschen** auswählen, dann geben Sie den Schlüsselalias in das Textfeld ein.
8. Wählen Sie **Schlüsselgruppe ändern** aus.
   Die Schlüsselgruppe wird geändert, um die Änderungen zu berücksichtigen.

Löschen von Schlüsselgruppen

Dieses Kapitel beschreibt das Löschen einer Schlüsselgruppe.

VORSICHT: Das Löschen einer Schlüsselgruppe löscht alle Schlüssel in dieser Schlüsselgruppe. Das Löschen eines Schlüssels entspricht dem Löschen aller Daten, die durch diesen Schlüssel geschützt wurden, da die Daten nicht länger zugänglich sind. Es gibt aus Sicherheitsgründen keine Möglichkeit, gelöschte Schlüssel wiederherzustellen.

ANMERKUNG: Die Standard-Schlüsselgruppe einer Gerätegruppe kann nicht gelöscht werden.

Führen Sie zum Löschen einer Schlüsselgruppe die folgenden Schritte durch:

1. Melden Sie sich am EKM 3.0 Portal an. Beziehen Sie sich auf Anmeldung am Encryption Key Manager 3.0 Portal.
   Es wird der Bildschirm **Willkommen bei Dell Encryption Key Manager** angezeigt.
2. Navigieren Sie im Navigationsfensterbereich zu **Dell Encryption Key Manager → Schlüssel- und Geräteverwaltung**.
   Es wird der Bildschirm **Schlüssel- und Geräteverwaltung** angezeigt.
3. Wählen Sie im Dropdown-Menü **Schlüssel und Geräte verwalten** den Gerätegruppennamen aus, zu dem Sie die Schlüsselgruppe hinzufügen wollen.
4. Klicken Sie neben **Schlüssel- und Geräteverwaltung** auf **Start**.
   Im **Schlüssel- und Geräteverwaltung**-Dienstprogramm wird eine Seite für die von Ihnen gewählte Gerätegruppe angezeigt. Diese Seite führt alle Schlüsselgruppen und Geräte auf, die zu dieser Gerätegruppe gehören.

5. Überprüfen Sie, dass die Schlüsselgruppe, die Sie löschen wollen nicht die Standard-Schlüsselgruppe ist. Wenn sie die Standard-Schlüsselgruppe ist, dann ändern Sie die Schlüsselgruppe so, dass diese nicht die Standard-Schlüsselgruppe ist:
   a) Klicken Sie in der Tabelle **Schlüsselgruppe** mit der rechten Maustaste auf die Schlüsselgruppe, die Sie löschen wollen.

      Ein Popup-Menü wird angezeigt.
   b) Wählen Sie im Popup-Menü **Bearbeiten**.

      Es wird das Unterfenster **Schlüsselgruppe ändern** angezeigt.
   c) Deaktivieren Sie das Kontrollkästchen **Zur Standardschlüsselgruppe machen**.
   d) Klicken Sie auf **Schlüsselgruppe ändern**.

      Es wird der Bildschirm **Schlüssel- und Geräteverwaltung** angezeigt.
6. Wählen Sie die Schlüsselgruppe, die Sie löschen wollen aus, um sie zu markieren und klicken Sie auf **Löschen**.

   Es wird ein Popup-Bestätigungsfenster angezeigt.
7. Klicken Sie im Popup-Fenster mit der Bestätigung auf **OK**.

   Die Schlüsselgruppe und alle der Gruppe zugeordneten Schlüssel werden gelöscht.

Überprüfung des Serverzertifikats

Dieses Kapitel beschreibt, wie Sie prüfen, ob das Serverzertifikat, das Sie verwenden wollen, das in Verwendung befindliche Zertifikat ist. Führen Sie dafür die folgenden Schritte durch:

1. Melden Sie sich am EKM 3.0 Portal an. Beziehen Sie sich auf Anmeldung am Encryption Key Manager 3.0 Portal.

   Es wird der Bildschirm **Willkommen bei Dell Encryption Key Manager** angezeigt.
2. Navigieren Sie im Navigationsfensterbereich zu **Dell Encryption Key Manager → Erweiterte Konfiguration → Serverzertifikate**.

   Es wird der Bildschirm **Serverzertifikate verwalten** angezeigt.
3. Vergewissern Sie sich, dass in der **In Verwendung**-Spalte für das Zertifikat, das Sie verwenden wollen ein Häkchen gesetzt wurde.

   *Wenn in der **In Verwendung**-Spalte für das gewünschte Zertifikat ein Häkchen gesetzt wurde*, ist dieses Verfahren abgeschlossen.

   *Wenn in der **In Verwendung**-Spalte für das gewünschte Zertifikat kein Häkchen gesetzt wurde*, dann führen Sie die folgenden Schritte durch:
   a) Klicken Sie auf das Zertifikat, das Sie verwenden wollen, um es zu markieren.
   b) Klicken Sie oben in der Tabelle auf **Ändern**.

      Es wird das Unterfenster **SSL/KMIP ändern** angezeigt.
   c) Aktivieren Sie das Kontrollkästchen **Derzeitiges Zertifikat in Verwendung**.
   d) Klicken Sie auf **Zertifikat ändern**.

      Es wird ein Popup-Fenster mit einer **Warnung** angezeigt.
   e) Klicken Sie im Popup-Fenster mit der **Warnung** auf **OK**.
   f) Stoppen Sie den Server und starten Sie ihn neu. Beziehen Sie sich auf Starten und Stoppen des EKM 3.0 Servers in Windows oder Starten und Stoppen des EKM 3.0 Servers in Linux..

ANMERKUNG: Außer der Einstellung eines Zertifikates als **In Verwendung** befindlich können Sie ein Zertifikat nicht ändern.

Anzeigen der Serverzertifikateinzelheiten

Wenn Sie die Zertifikateinzelheiten anzeigen wollen, dann führen Sie die folgenden Schritte durch:

1. Klicken Sie auf das Zertifikat, um es zu markieren.
2. Klicken Sie oben in der Tabelle auf **Ändern**.
   Es wird das Unterfenster **SSL/KMIP-Zertifikat ändern** angezeigt.
3. Zeigen Sie die Zertifikatdetails an. Sie können auch auf **Optionale Zertifikatparameter** klicken, um etwaige optionale Parameter anzuzeigen.

Anmeldung am WebSphere-Server

Für einige Verfahren in dieser Anleitung ist es erforderlich, dass Sie sich am WebSphere-Server anmelden. Dieses Kapitel beschreibt die Anmeldung am WebSphere-Server in Windows und Linux. Sie müssen sich nur dann am WebSphere-Server anmelden, wenn Sie in einem weiteren Verfahren dazu angewiesen werden.

So melden Sie sich mit dem **wsadmin**-Befehl am WebSphere-Server an:

1. Navigieren Sie *in Windows* in einer Eingabeaufforderung zu ***<Stammverzeichnis>:\Dell\EKM\bin***. Navigieren Sie *in Linux* in einer Terminalsitzung zu **/opt/dell/ekm/bin**.
2. Geben Sie *für Windows* folgenden Befehl ein:
   ```
   wsadmin -username tklmadmin -password <tklm password> -lang jython
   ```
   Geben Sie *für Linux* folgenden Befehl ein:
   ```
   ./wsadmin.sh -username tklmadmin -password <tklm password> -lang jython
   ```
   Drücken Sie **Eingabe**. Der Befehl wird für kurze Zeit ausgeführt und es wird die **wsadmin** Eingabeaufforderung angezeigt.

ANMERKUNG: Die Befehle unterscheiden zwischen Groß- und Kleinschreibung. Um Klammern herum gibt es keine Leerzeichen. Geben Sie um Variablen herum keine „Größer als" bzw. „Kleiner als"-Symbole (< >) ein.

ANMERKUNG: Geben Sie für die Abmeldung vom WebSphere-Server **Beenden** ein und drücken Sie **Eingabe**.

Starten und Stoppen des EKM 3.0 Servers in Windows

Dieses Kapitel beschreibt das Starten und Stoppen des EKM 3.0 Servers in Windows.

1. Navigieren Sie in einer Eingabeaufforderung zu ***<Stammverzeichnis>*:\Dell\EKM\bin**.
2. Geben Sie zum Starten des Servers den folgenden Befehl ein:
   ```
   startserver server1
   ```
   Geben Sie zum Stoppen des Servers den folgenden Befehl ein:
   ```
   stopserver server1
   ```
3. Drücken Sie die **Eingabetaste.**
   Der Befehl wird ausgeführt und die Eingabeaufforderung zeigt diese Bestätigungsmeldung an:
   ```
   Server server1 open for e-business (Server server 1 steht für E-Business
   zur Verfügung)
   ```
   oder
   ```
   Server server1 stop completed (Server server 1 Stoppen abgeschlossen)
   ```

Starten und Anhalten des EKM 3.0 Servers in Linux

Dieses Kapitel beschreibt das Starten und Stoppen des EKM 3.0 Servers in Linux.

ANMERKUNG: Sie müssen sich zum Starten und Stoppen des Servers als Root-Benutzer anmelden.

1. Navigieren Sie in einer Terminalsitzung zu **/opt/dell/ekm/bin**.
2. Geben Sie zum Starten des Servers den folgenden Befehl ein:
   ```
   ./startserver.sh server1
   ```
   Geben Sie zum Stoppen des Servers den folgenden Befehl ein:
   ```
   ./stopserver.sh server1
   ```

   ANMERKUNG: Sie werden zum Stoppen des Servers zur Eingabe der EKM 3.0 Administrator-Anmeldedaten aufgefordert.
3. Drücken Sie die **Eingabetaste.**
   Der Befehl wird ausgeführt und die Terminalsitzung zeigt diese Bestätigungsmeldung an:
   ```
   Server server1 open for e-business (Server server 1 für E-Business geöffnet)
   ```
   oder
   ```
   Server server1 stop completed (Server server 1 Stoppen abgeschlossen)
   ```

6

Migration und Zusammenführung

Während der EKM 3.0 Installation können Sie EKM 2.X in EKM 3.0 migirieren.

Nach der EKM 3.0 Installation können Sie EKM 2.X in EKM 3.0 zusammenführen.

Dieses Kapitel beschreibt die Zusammenführungs- und Migrationsverfahren.

ANMERKUNG: Es können nur EKM 2.X-Versionen migiriert oder zusammengeführt werden, die zur Erstellung von Schlüsseln verwendet wurden.

Migration einer Encryption Key Manager (EKM) 2.X-Version während der EKM 3.0-Installation

Führen Sie dieses Verfahren nur durch, wenn Sie während der EKM 3.0-Installation den Bildschirm **Migration** konfigurieren. Der Bildschirm **Migration** wird dazu verwendet, eine Encryption Key Manager (EKM) 2.X-Version in EKM 3.0 zu migrieren.

ANMERKUNG: Wenn Sie derzeit EKM 2.X verwenden, empfiehlt Dell, dass Sie Ihre derzeitige Infrastruktur beibehalten (Server, Betriebssysteme, Band-Libraries, etc. die von EKM 2.X geschützt werden), wenn keine Probleme auftreten.

Wenn Sie eine EKM 2.X-Version in EKM 3.0 migrieren müssen, empfiehlt Dell, dass Sie diese jetzt migrieren.

ANMERKUNG: Wenn Sie EKM 2.X mit einer Virtual Machine als EKM 2.X-Host verwenden, müssen Sie auf EKM 2.X bleiben, oder auf einen physikalischen Server migrieren. EKM 3.0 unterstützt keine Virtual Machines als Hosts.

ANMERKUNG: Während der EKM 3.0-Installation können Sie nur eine einzige EKM 2.X-Version migrieren. Wenn Sie mehr als eine EKM 2.X-Version für die Portierung auf EKM 3.0 haben, dann migrieren Sie die erste unter Verwendung dieses Verfahrens und beziehen Sie sich nach Abschluss der Installation auf Zusammenführung weiterer EKM 2.X-Versionen in EKM 3.0, um die zusätzlichen Versionen zusammenzuführen.

Es ist möglich, die EKM 2.X-Version in EKM 3.0 *zusammenzuführen*, nachdem die EKM 3.0-Installation unter Verwendung des EKM 2.X auf EKM 3.0-Zusammenführungstools abgeschlossen wurde, jedoch empfiehlt Dell nachdrücklich, dass Sie die Migration zum jetzigen Zeitpunkt durchführen.

ANMERKUNG: Wenn Sie eine EKM 3.0-Primär/Sekundärserverkonfiguration verwenden, dann müssen Sie das Migrationsverfahren nur auf dem primären EKM 3.0-Server durchführen.

Führen Sie nach Abschluss der Migration eine Sicherung des primären EKM 3-Servers durch und verwenden Sie die Sicherung, um den sekundären EKM 3.0-Server wiederherzustellen, damit dieser zum primären EKM 3-Server passt.

Fahren Sie fort mit EKM 2.X auf EKM 3.0 Migrationsverfahren, um während des EKM 3.0-Installationsvorgangs von EKM 2.0 zu migrieren.

Migrationsverfahren für EKM 2.X auf EKM 3.0

Führen Sie die folgenden Schritte aus, um während der EKM 3.0-Installation eine EKM 2.X-Version vom Bildschirm **Migration** aus auf EKM 3.0 zu migirieren:

1. Melden Sie sich an der EKM 2.X-Konsole an, sichern Sie den EKM 2.X Keystore, stoppen Sie den EKM 2.X und beenden Sie die EKM 2.X-Konsole. Beziehen Sie sich für weitere Informationen auf das EKM 2.X-Benutzerhandbuch.
2. Kopieren Sie den EKM 2.X-Ordner:

   Wenn der EKM 2.X Server auf einem anderen Computer als dem Computer, auf dem EKM 3.0 installiert werden soll installiert ist, dann kopieren Sie den EKM 2.X-Ordner des EKM 2.X-Servers in einen temporären Ordner auf dem EKM 3.0 Server (beispielsweise **C:\temp\MyEKM2** in Windows, oder **/opt/myekm2** in Linux).

   Wenn der EKM 2.X Server auf dem gleichen Computer wie dem Computer, auf dem EKM 3.0 installiert werden soll installiert ist, müssen Sie dennoch eine Kopie des EKM 2.X-Ordners auf diesem Computer erstellen.
3. Setzen Sie auf dem Bildschirm **Migration** der EKM 3.0 Installation ein Häkchen in das Kontrollkästchen **Migration von EKM 2.X auf EKM 3.0**.
4. Klicken Sie auf **Auswahl** und navigieren Sie in das Verzeichnis, in das Sie zuvor den EKM 2.X-Ordner kopiert haben. Wählen Sie außer diesem Ordner nichts anderes aus.

VORSICHT: Wenn EKM 2.X Server auf dem gleichen Computer wie dem Computer, auf dem EKM 3.0 installiert werden soll installiert ist, dann navigieren Sie nicht in das Verzeichnis, in dem EKM 2.X installiert ist, weil das EKM 3.0-Installationsprogramm den für die Migration verwendeten Ordner löscht. Navigieren Sie zur Kopie des EKM2.X-Verzeichnisses, die Sie zuvor erstellt haben.

5. Klicken Sie auf **Weiter**.

   Der Bildschirm **Konfigurations-Zusammenfassung** wird angezeigt.

ANMERKUNG: Wenn eine Fehlermeldung angezeigt wird, dann überprüfen Sie den Pfad Ihres EKM 2.X - Verzeichnisses.

6. Fahren Sie mit der EKM 3.0-Installation fort. Beziehen Sie sich auf Durchführung des EKM 3.0 Installationsverfahrens.

ANMERKUNG: Das Kennwort für den neuen EKM 3.0 Keystore ist das gleiche Kennwort, das dem für die Migration verwendeten EKM 2.X Keystore zugeordnet wurde.

VORSICHT: Führen Sie EKM 2.X nicht aus, nachdem Sie seine Schlüssel auf EKM 3.0 migriert haben. Falls geünscht, können Sie die EKM 2.X-Dateien nach der erfolgreichen Migration von EKM 2.X auf EKM 3.0. sichern. Dell empfiehlt die Sicherung der EKM 2.X-Dateien, bevor Sie EKM 2.X deinstallieren.

Zusammenführung von Encryption Key Manager (EKM) 2.X in EKM 3.0 nach der Installation von EKM 3.0

Dieses Kapitel beschreibt das EKM 2.0 in EKM 3.0-Zusammenführungsverfahren nach der Installation für Windows und Linux. Dieses Verfahren verwendet das EKM 2.X auf EKM 3.0-Zusammenführungstool.

Verwenden Sie dieses Verfahren, wenn EKM 3.0 bereits installiert und konfiguriert wurde und Sie EKM 2.X in EKM 3.0 zusammenführen wollen.

ANMERKUNG: Wenn Sie eine EKM 3.0-Primär/Sekundärserverkonfiguration verwenden, dann müssen Sie das Migrationsverfahren nur auf dem primären EKM 3.0-Server durchführen. Führen Sie nach Abschluss der Zusammenführungsverfahrens auf dem primären EKM 3.0-Server das Wiederherstellungsverfahren durch und stellen Sie die Sicherungsdatei auf dem sekundären EKM 3.0-Server wieder her. Beziehen Sie sich auf Durchführen von Sicherungen und Wiederherstellen aus einer Sicherung..

ANMERKUNG: Falls EKM 3.0 noch nicht installiert wurde, empfiehlt Dell die Migration von EKM 2.X in EKM 3.0 während der EKM 3.0-Installation. Beziehen Sie sich auf Durchführung des EKM 3.0 Installationsverfahrens.

Die Beispiele in diesem Dokument verwenden die standardmäßigen Windowspfade (zum Beispiel **C:\<*Ordnername*>**). Ersetzen Sie diese mit dem entsprechenden Stammlaufwerksbuchstaben bzw. Linux-Pfad Ihres Systems.

Zusammenführungstool-Voraussetzungen

Überprüfen Sie vor dem Ausführen des Zusammenführungstools, ob die folgenden Anforderungen erfüllt werden:

- EKM 3.0 muss installiert sein und der Master-Keystore muss erstellt worden sein, anderenfalls schlägt das Zusammenführungsverfahren fehl. Beziehen Sie sich auf Erstellung eines Master-Keystores.
- Bei der Zusammenführung von EKM 2.X auf EKM 3.0 müssen EKM 2.X und EKM 3.0 auf der gleichen Betriebssystemversion installiert sein.
- Wenn Sie zuvor EKM 2.X in EKM 3.0 zusammengeführt oder migriert haben, ist das **ekmcert-Zertifikat** der vorherigen Zusammenführung oder Migration auf dem EKM 3.0-Server nach wie vor vorhanden und möglicherweise immer noch vorhanden, nachdem Sie aus einer vorherigen Sicherung wiederhergestellt haben. Sie müssen das **ekmcert-**Zertifikat vom EKM 3.0-Server entfernen, bevor Sie das Zusammenführungsverfahren durchführen. Beziehen Sie sich auf Löschen des ekmcert-Zertifikats, der Schlüssel, Schlüsselgruppen und Umbenennung von Geräten.
- Sie müssen die Duplikate von Schlüsseln, Schlüsselgruppen und Geräten in EKM 2.X umbenennen, bevor Sie diese in EKM 3.0 zusammenführen. Beziehen Sie sich auf das EKM 2.X Benutzehandbuch.
  - Bei EKM 2.X als Quelle und EKM 3.0 als Ziel dürfen keine Duplikate von Schlüsselalias/namen vorhanden sein. Jeder eingehende Schlüssel muss einen eindeutigen Alias/Namen haben, anderenfalls schlägt das Zusammenführungsverfahren fehl.
  - Bei EKM 2.X als Quelle und EKM 3.0 als Ziel dürfen keine Duplikate von Schlüssel*gruppen*alias/namen vorhanden sein. Jede eingehende Schlüsselgruppe muss einen eindeutigen Alias/Namen haben, anderenfalls schlägt das Zusammenführungsverfahren fehl.
  - Bei EKM 2.X als Quelle und EKM 3.0 als Ziel dürfen keine Duplikate von Geräten vorhanden sein, anderenfalls schlägt das Zusammenführungsverfahren fehl.

EKM 2.X auf EKM 3.0 Zusammenführungsverfahren

Führen Sie die folgenden Schritte zum Ausführen des Zusammenführungstools durch:

1. Melden Sie sich am EKM 3.0 Portal an. Beziehen Sie sich auf Anmeldung am Encryption Key Manager 3.0 Portal.

   Es wird der Bildschirm **Willkommen bei Dell Encryption Key Manager** angezeigt.
2. Erstellen Sie auf dem EKM 3.0 Server eine Sicherung von EKM 3.0. Beziehen Sie sich für das Verfahren zum Erstellen von Sicherungen auf Durchführen von Sicherungen und Wiederherstellen aus einer Sicherung.

   Wenn das Zusammenführungstool fehlschlägt oder EKM 3.0-Daten beschädigt, können Sie die Sicherung verwenden, um jegliche verlorengegangenen Informationen wiederherzustellen.
3. Melden Sie sich aus EKM 3.0 ab.
4. Stoppen Sie den EKM 3.0-Server vor dem Ausführen des Zusammenführungstools. Beziehen Sie sich auf Starten und Stoppen des EKM 3.0 Servers in Windows oder Starten und Stoppen des EKM 3.0 Servers in Linux.
5. Erstellen Sie im Stammverzeichnis des EKM 3.0 Servers einen geeigneten Ordner (z.B. **C:\EKM_Files** in Windows, oder **/opt/EKM_Files** in Linux).
6. Melden Sie sich an der EKM 2.X-Konsole an, sichern Sie den EKM 2.X-Keystore, stoppen Sie den EKM 2.X-Server und beenden Sie die EKM 2.X-Konsole. Beziehen Sie sich auf das EKM 2.X-Benutzerhandbuch.
7. Kopieren Sie die folgenden Dateien aus dem Speicherort, in dem EKM 2.X installiert ist in den Ordner, den Sie im vorherigen Schritt auf dem EKM 3.0 Server erstellt haben. Wenn EKM 2.X auf einem anderen physikalischen System installiert ist, dann verwenden Sie ein Wechsellaufwerk oder eine Serverfreigabe mit dem gleichen Betriebssystem.
   - Kopieren Sie in Windows aus **<*Stammverzeichnis*>:\ekm\gui\ EKMKeys.jck**. In Linux befindet sich diese in **/var/ekm/gui**.
   - Kopieren Sie in Windows aus **<*Stammverzeichnis*>:\ekm\gui\ KeyManagerConfig.properties** (dies ist die EKM-Konfigurationsdatei). In Linux befindet sich diese in **/var/ekm/gui**.

- Kopieren Sie in Windows aus **<*Stammverzeichnis*>:\ekm\gui\ keygroup.xml**. In Linux befindet sich diese in **/var/ekm/gui/keygroups**.
- Kopieren Sie in Windows aus **<*Stammverzeichnis*>:\ekm\gui\drivetable\ ekm_drivetable.dt**. In Linux befindet sich diese in **/var/ekm/gui/drivetable**.

VORSICHT: Verwenden Sie in Windows Notepad zum Erstellen oder Bearbeiten von Dateien. Wenn Sie Wordpad verwenden, schlägt dieses Verfahren fehl.

8. Bearbeiten Sie die Datei **KeyManagerConfig.properties**, sodass diese nur die folgenden Eigenschaften enthält:

   - **config.keygroup.xml.file**
   - **config.keystore.password.obfuscated**
   - **config.keystore.file**
   - **config.drivetable.file.url**

   Löschen Sie die übrigen Zeilen. Beziehen Sie sich in diesem Verfahren z.B. auf Code-Beispiel.

9. Fügen Sie die folgenden DB2-Optionen zur neuen **KeyManagerConfig.properties**-Datei hinzu:

   - jdbcURL = jdbc:db2://localhost:<*EKM 3.0 DB2 Datenbankport*>/<*EKM 3.0 DB2 Datenbankname*>

     oder

     jdbcURL = jdbc:db2://<*EKM 3.0 Server IP-Adresse*>:<*EKM 3.0 DB2 Datenbankport*>/<*EKM 3.0 DB2 Datenbankname*>
   - jdbcUID = <*DB2 Administratorbenutzername*>
   - jdbcPW = <*DB2 Administratorkennwort*>
   - dbType = DB2

   Beziehen Sie sich z.B. auf Code-Beispiel, um ein Beispiel für dieses Verfahren zu erhalten.

ANMERKUNG: Die Variablen sind Parameter, die Sie eingestellt haben, als Sie EKM 3.0 installiert haben. Geben Sie um Variablen herum keine „Größer als“ und „Kleiner als“-Symbole (< >) ein. Bei Variablen, Benutzernamen und Kennwörtern wird zwischen Groß- und Kleinschreibung unterschieden.

10. Fügen Sie den Kennworteintrag für den EKM 3.0 Standard-Keystore zur Datei **KeyManagerConfig.properties** hinzu. Der Kennworteintrag lautet:

    tklm.encryption.password = <*ekm 3.0 keystore password*>.

    Die aktualisierte **KeyManagerConfig.properties**-Datei sollte ähnlich wie in folgendem Beispiel aussehen:

Code-Beispiel für Windows

```
config.keygroup.xml.file = File:c:\\<EKM_Files>\\KeyGroups.xml
config.keystore.password.obfuscated = 38087C9DA4A4696A6B6C
config.keystore.file = c:\\<EKM_Files>\\EKMKeys.jck
config.drivetable.file.url = File:c:\\<EKM_Files>\
\ekm_drivetable.dt jdbcURL = jdbc:db2://localhost:50010/ekm_dell
jdbcUID = ekmdell1 jdbcPW = Dell1234 dbType = DB2
tklm.encryption.password = Dell1234
```

Wobei *EKM_Files* der von Ihnen zuvor erstellte Ordner ist.

Code-Beispiel für Linux

```
config.keygroup.xml.file = File:/opt/<EKM_Files>/KeyGroups.xml
config.keystore.password.obfuscated = 38087C9DA4A4696A6B6C
config.keystore.file = /opt/<EKM_Files>/EKMKeys.jck
config.drivetable.file.url = File:/opt/<EKM_Files>/
ekm_drivetable.dt jdbcURL = jdbc:db2://localhost:50010/ekm_dell
jdbcUID = ekmdell1 jdbcPW = Dell1234 dbType = DB2
tklm.encryption.password = Dell1234
```

Wobei *EKM_Files* der zuvor von Ihnen erstellte Ordner ist.

11. Navigieren Sie zum Ordner **EKM2DKMMerge** auf dem EKM 3.0 Installationsdatenträger. Kopieren Sie aus dem Ordner **EKM2DKMMerge** die Datei **EKM2DKMMerge.jar** in den von Ihnen zu Anfang des Verfahrens erstellten Ordner (beispielsweise C:\EKM_Files in Windows, oder /opt/EKM_Files in Linux).

ANMERKUNG: Sie müssen für alle folgenden Schritte die gleiche Eingabeaufforderungs- oder Terminalsitzung verwenden. Wenn Sie Eingabeaufforderungs- oder Terminalsitzungen ändern, wird der von Ihnen festgelegte CLASSPATH nicht automatisch auf andere Eingabeaufforderungs- oder Terminalsitzungen angewendet.

12. Konfigurieren Sie auf dem EKM 3.0 Server die von dem Zusammenführungstool benötigten Pfade für WAS und TIP.

    In Windows:

    a. Navigieren Sie in einer Eingabeaufforderung zu **<*Stammverzeichnis*>:\Dell\EKM\bin**.

    b. Geben Sie zum Ausführen des Befehlszeilenskripts den folgenden Befehl ein:

    ```
    setupCmdLine.bat
    ```

    Beispiel:

    ```
    C:\Dell\EKM\bin\setupCmdLine.bat
    ```

    c. Drücken Sie **Eingabe**. Der Befehl wird ausgeführt und das System zeigt in der letzten Zeile den folgenden Text an:

    ```
    goto :EOF
    ```

    In Linux:

    a. Navigieren Sie in einer Terminalsitzung zu **/opt/dell/ekm/bin**.

    b. Geben Sie folgenden Befehl ein:

    ```
    . setupCmdLine.sh
    ```

    c. Der Befehl wird ausgeführt. Nach erfolgreichem Abschluss des Befehls in Linux wird eine leere Eingabeaufforderung angezeigt. Auf den Abschluss des Befehls wird nicht hingewiesen.

ANMERKUNG: Das Skript **setupCmdLine.sh** muss über Ausführungsberechtigungen verfügen.

13. Erstellen Sie eine Befehlszeilenstapelverarbeitungsdatei (Batch-Datei) (.bat, in Linux .sh), um die durch das Zusammenführungstool benötigten .jar-Dateien zu beschaffen und um zusätzliche Parameter für den CLASSPATH einzustellen:

    a) Kopieren Sie das folgende temporäre CLASSPATH-Setup in eine Textdatei und benennen Sie diese mit *<Dateiname>*.bat oder in Linux mit *<Dateiname>*.sh (z.B. **setupclasspath.bat** in Windows, oder **setupclasspath.sh** in Linux).

    b) Speichern Sie die .bat/.sh-Datei im Ordner, den Sie zu Anfang dieses Verfahrens erstellt haben, z.B. C:\EKM_Files oder /opt/EKM_Files.

VORSICHT: Verwenden Sie in Windows Notepad zum Erstellen oder Bearbeiten von Dateien. Wenn Sie Wordpad verwenden, schlägt dieses Verfahren fehl.

    c) Bearbeiten Sie die Stapeldatei:

    Bearbeiten Sie in Windows die Stapelverarbeitungsdatei, um ***c:\EKM\Needed*** durch den Pfad zu ersetzen, in dem Sie die Datei **EKM2DKMMerge.jar** platziert haben, z.B. **c:\EKM_Files**.

    Bearbeiten Sie in Linux, das Shell-Skript, um **/opt/EKM_Files** durch den Pfad zu ersetzen, in dem Sie die Datei **EKM2DKMMerge.jar** platziert haben.

    Temporäres CLASSPATH-Setup für Windows

    ```
    set JAVA_HOME=%WAS_HOME%\java set PATH=%JAVA_HOME%\bin;%JAVA_HOME%\jre
    \bin;%PATH% set CLASSPATH=c:\EKM\Needed\EKM2DKMMerge.jar;%CLASSPATH% set
    CLASSPATH=.;%WAS_HOME%\plugins\com.ibm.icu_3.4.5.jar;%WAS_HOME%\products
    \tklm\migration\j2ee.jar;%WAS_HOME%\plugins\com.ibm.tklm.commands.jar;
    %WAS_HOME%\products\tklm\migration\com.ibm.tklm.kmip.adapter.jar;%WAS_HOME
    %\profiles\TIPProfile\installedApps\TIPCell\tklm_kms.ear
    \com.ibm.tklm.kmip.jar;"C:\Program Files\Dell\db2dkm\java\db2jcc.jar";"C:
    \Program Files\Dell\db2dkm\java\db2jcc_license_cu.jar";%WAS_HOME%\profiles
    ```

```
\TIPProfile\installedApps\TIPCell\tklm_kms.ear\com.ibm.tklm.keyserver.jar;
%WAS_HOME%\profiles\TIPProfile\installedApps\TIPCell\tklm_kms.ear
\com.ibm.tklm.server.api.jar;%WAS_HOME%\profiles\TIPProfile\installedApps
\TIPCell\tklm_kms.ear\com.ibm.tklm.server.db.ejb.jar;%CLASSPATH%
```

ANMERKUNG: Ersetzen Sie die Laufwerksbuchstaben wie erforderlich.

ANMERKUNG: Wenn Sie eine 64-Bit Version von WIndows verwenden, dann bearbeiten Sie die Stapelverarbeitungsdatei, um im obigen CLASSPATH **Programme** durch **Programme (x86)** zu ersetzen.

Temporäres CLASSPATH-Setup für Linux

```
export JAVA_HOME=$WAS_HOME/java export PATH=${JAVA_HOME}/bin:${JAVA_HOME}
$/jre/bin:$PATH export CLASSPATH=/opt/EKM_Files/EKM2DKMMerge.jar:
$CLASSPATH export CLASSPATH=.:$WAS_HOME/plugins/com.ibm.icu_3.4.5.jar:
$WAS_HOME/products/tklm/migration/j2ee.jar:$WAS_HOME/plugins/
com.ibm.tklm.commands.jar:$WAS_HOME/products/tklm/migration/
com.ibm.tklm.kmip.adapter.jar:$WAS_HOME/profiles/TIPProfile/installedApps/
TIPCell/tklm_kms.ear/com.ibm.tklm.kmip.jar:/opt/dell/db2ekm/java/
db2jcc.jar:/opt/dell/db2ekm/java/db2jcc_license_cu.jar:$WAS_HOME/profiles/
TIPProfile/installedApps/TIPCell/tklm_kms.ear/com.ibm.tklm.keyserver.jar:
$WAS_HOME/profiles/TIPProfile/installedApps/TIPCell/tklm_kms.ear/
com.ibm.tklm.server.api.jar:$WAS_HOME/profiles/TIPProfile/installedApps/
TIPCell/tklm_kms.ear/com.ibm.tklm.server.db.ejb.jar:$CLASSPATH
```

14. Führen Sie die gerade erstellte Stapelverarbeitungsdatei aus. Navigieren Sie in der gleichen Eingabeaufforderung bzw. Terminalsitzung auf dem EKM 3.0 Server in den von Ihnen zu Anfang des Verfahrens erstellten Ordner (z.B. C:\EKM_Files in Windows, oder /opt/EKM_Files in Linux) und führen Sie die Stapelverarbeitungsdatei aus, die Sie im vorherigen Schritt erstellt haben. Lokalisieren Sie in Linux die zuvor erstellte Datei, z.B. setupclasspath.sh.
15. Führen Sie auf dem EKM 3.0 Server in der gleichen Eingabeaufforderung oder Terminalsitzung den folgenden Java-Befehl aus:

```
java<space>com.ibm.tklm.ekm2tklm.MergeEKM2KLM<space>KeyManagerConfig.propert
ies
```

ANMERKUNG: Bei den Befehlen wird zwischen Groß- und Kleinschreibung unterschieden. Geben Sie um Variablen herum keine „Größer als“ und „Kleiner als“-Symbole (< >) ein.

Die Datei **KeyManagerConfig.properties** ist die Datei, die Sie zu Anfang dieses Verfahrens aktualisiert haben.

Dieser Befehl führt EKM 2.X mit EKM 3.0 zusammen.

Bei erfolgreichem Abschluss wird die folgende Meldung angezeigt:

```
TKLM version: 2.0.0.0 201007241325Starting EKM to KLM MergeKMSDebug.init,
debug output filename not specified: using defaultCTGKS0250I: Successfully
migrated the Encryption Key Manager keystores, certificates and
keys.CTGKS0251I: Successfully migrated the Encryption Key Manager key
groups.CTGKS0249I: Successfully migrated the Encryption Key Manager
devices.Migration Complete.
```

ANMERKUNG: Wenn Sie Fehler erhalten, dann zeigen Sie das Debugprotokoll an, um die Ursache dafür zu bestimmen. Falls gewünscht, können Sie das Debugprotokoll in einem anderen Speicherort speichern, oder es umbenennen, sodass es statisch gemacht wird, da anderenfalls das EKM 2.X auf EKM 3.0-Zusammenführungsprotokoll Daten anhängt. In Windows befindet sich das Debugprotokoll in folgendem Verzeichnis des EKM 3.0 Servers: ***<Stammverzeichnis>*:\Dell\EKM\bin\products\tklm\logs\debug.log**. In Linux befindet sich das Debugprotokoll in folgendem Verzeichnis des EKM 3.0 Servers: **/opt/dell/ekm/bin/products/tklm/logs/debug.log**.

ANMERKUNG: Wenn Sie den folgenden Fehler erhalten, dann versuchen Sie zu migirieren, während ein doppeltes Element auf dem EKM 2.X Server und EKM 3.0 Server vorhanden ist .

```
Duplicate <item> = <item>Migration failed. Please refer to the debug file
for more information. (Doppelt vorhanden <Element> = <Element>Migration
fehlgeschlagen. Bitte beziehen Sie sich für weitere Informationen auf die
Debugdatei.)
```

Beziehen Sie sich auf Löschen der ekmcert-Zertifikate, Schlüssel und Schlüsselgruppen, sowie Geräte umbenennen

Wenn Sie den folgenden Fehler erhalten und Sie den Schlüssel löschen wollen, anstelle ihn umzubenennen, dann schließen Sie die Eingabeaufforderung bzw. Terminalsitzung nicht. Sie müssen den Schlüsselalias aus der Eingabeaufforderung bzw. Terminalsitzung kopieren.

```
Duplicate Key Alias= <key alias>
```

Beziehen Sie sich auf Löschen der ekmcert-Zertifikate, Schlüssel und Schlüsselgruppen, sowie Geräte umbenennen.

VORSICHT: Das Löschen eines Schlüssels entspricht dem Löschen aller Daten, die durch diesen Schlüssel geschützt werden, da die Daten nicht mehr zugänglich sind. Aus Sicherheitsgründen besteht keine Möglichkeit, gelöschte Schlüssel wiederherzustellen.

16. Starten Sie den EKM 3.0-Server unter Verwendung des **startserver**-Befehls. Beziehen Sie sich auf Starten und Stoppen des EKM 3.0 Servers in Windows oder Starten und Stoppen des EKM 3.0 Servers in Linux.
17. Überprüfen Sie, ob die EKM 2.X-Schlüsselgruppen, Schlüssel und Geräte auf EKM 3.0 migriert wurden. Beziehen Sie sich auf Prüfen der EKM 2.X auf EKM 3.0 Zusammenführung oder Migration. Wenn der Zusammenführungsvorgang erfolgreich war, ist das Verfahren abgeschlossen. Wenn Sie weitere EKM 2.X Versionen auf EKM 3.0 zusammenführen wollen, dann beziehen Sie sich auf Zusammenführung weiterer EKM 2.X Versionen auf EKM 3.0. Wenn der Zusammenführungsvorgang nicht erfolgreich war, dann beziehen Sie sich auf Zusammenführung fehlgeschlagen.

VORSICHT: Führen Sie EKM 2.X nicht aus, nachdem Sie seine Schlüssel auf EKM 3.0 zusammengeführt haben. Falls gewünscht, können Sie EKM 2.X nach der erfolgreichen Zusammenführung von EKM 2.X auf EKM 3.0 deinstallieren. Dell empfiehlt die Sicherung der EKM 2.X-Dateien, bevor Sie EKM 2.X deinstallieren.

Überprüfen der EKM 2.X auf EKM 3.0 Zusammenführung oder Migration

Dieses Kapitel beschreibt, wie Sie überprüfen, ob die EKM 2.X auf EKM 3.0 Zusammenführungs- oder Migrationsverfahren erfolgreich waren und ob die Band-Libraries funktionsfähig sind.

Führen Sie die folgenden Schritte durch, um zu prüfen, ob der EKM 2.X erfolgreich in EKM 3.0 zusammengeführt oder migriert wurde:

1. Melden Sie sich am EKM 3.0-Portal an. Beziehen Sie sich auf Anmeldung am Encryption Key Manager 3.0 Portal.
   Es wird der Bildschirm **Willkommen bei Dell Encryption Key Manager** angezeigt.
2. Navigieren Sie im Navigationsfensterbereich zu **Dell Encryption Key Manager → Schlüssel- und Geräteverwaltung**.
   Es wird der Bildschirm **Schlüssel- und Geräteverwaltung** angezeigt.
3. Wählen Sie im Dropdown-Menü **Schlüssel und Geräte verwalten LTO** aus und klicken Sie auf **Start**.
   Der Bildschirm **Schlüssel- und Geräteverwaltung** zeigt die migrierte(n) EKM-Schlüsselgruppe(n) und die Anzahl der Schlüssel in jeder Gruppe an.
4. Wählen Sie im Dropdown-Menü oben in der Tabelle **Schlüssel, Schlüsselgruppenmitgliedschaft und Laufwerke anzeigen** aus. Wenn in der linken Tabellenseite Schlüssel angezeigt werden, war die Zusammenführung erfolgreich.

5. Die Migration importiert keine EKM 2.0-konfigurierten Geräte. Sie müssen die EKM 2.X-Geräte konfigurieren. Beziehen Sie sich auf Hinzufügen eines Gerätes zu einer Gerätegruppe.
6. Überprüfen Sie im EKM 3.0-Portal, ob EKM 3.0 für das automatische Annehmen von Geräteanfragen konfiguriert ist. Die Einstellung auf dem Bildschirm **Schlüssel- und Geräteverwaltung** sollte **Automatische Annahme aller neuen Geräte-Kommunikationsanfragen** lauten.
7. Überprüfen Sie die Geräte in Ihrer Library:
   a) Überprüfen Sie, ob der SSL-Port und TCP-Port korrekt für Ihre Band-Library konfiguriert wurden.
   b) Führen Sie von Ihrer Band-Library aus Schlüsselpfaddiagnosen aus, um die Konfiguration der Band-Library zu überprüfen.

ANMERKUNG: Beziehen Sie sich für weitere Informationen auf das Benutzerhandbuch der Band-Library. Lesen Sie den Abschnitt „Dokumentation und Referenzmaterialien" der Datei **ReadThisFirst.txt** auf dem EKM 3.0 Installationsdatenträger, um Informationen zum Ausfindigmachen der Band-Library zu erhalten.

Zusammenführungsfehler

Wenn das Zusammenführungsverfahren fehlschägt, dann führen Sie die folgenden Schritte durch:

1. Prüfen Sie, ob der EKM 3.0 Server gestartet wurde. Wenn nicht, starten Sie den EKM 3.0 Server unter Verwendung des **startserver**-Befehls. Beziehen Sie sich auf Starten und Stoppen des EKM 3.0 Servers in Windows oder Starten und Stoppen des EKM 3.0 Servers in Linux.
2. Schließen Sie die Eingabeaufforderung.
3. Erfassen Sie das Debugprotokoll, indem Sie es in einem anderen Speicherort speichern oder es umbenennen.
   Das Debugprotokoll befindet sich in folgendem Verzeichnis: ***<Stammverzeichnis>*:\Dell\EKM\bin\products\tklm\logs\debug.log** in Windows, bzw. **/opt/dell/ekm/bin/products/tklm/logs/debug.log** in Linux.
4. Stellen Sie EKM 3.0 durch das EKM 3.0 Portal aus der Sicherung wieder her, die Sie im ersten Schritt von EKM 2.X auf EKM 3.0 Zusammenführungsverfahren erstellt haben. Beziehen Sie sich für Anweisungen für das Wiederherstellen aus einer Sicherung auf Wiederherstellen aus einer Sicherung.
5. Führen Sie das Zusammenführungsverfahren erneut durch. Beziehen Sie sich auf EKM 2.X auf EKM 3.0 Zusammenführungsverfahren.

Zusammenführung von zusätzlichen EKM 2.X Versionen mit EKM 3.0

Führen Sie dieses Verfahren durch, wenn Sie EKM 2.X in EKM 3.0 migiriert oder zusammengeführt haben und weitere EKM 2.X Versionen mit EKM 3.0 zusammenführen wollen.

1. Entfernen Sie das **ekmcert-Zertifikat** aus EKM 3.0. Beziehen Sie sich auf Löschen des ekmcert -Zertifikats, der Schlüssel und Schlüsselgruppen und Umbenennung von Geräten.
2. Führen Sie das Zusammenführungsverfahren für jede weitere EKM 2.X Version durch, die Sie zusammenführen wollen. Beziehen Sie sich auf EKM 2.X in EKM 3.0 Zusammenführungsverfahren.

Löschen des ekmcert-Zertifikats, der Schlüssel und Schlüsselgruppen und Umbenennen von Geräten

Bei der Durchführung einer EKM 2.X auf EKM 3.0-Zusammenlegung dürfen in EKM 2.X und auf dem EKM 3.0 Server keine Duplikate von **ekmcert-Zertifikaten,** Schlüsselaliase, oder Geräte vorhanden sein.

ANMERKUNG: Wenn Duplikate von Schlüsseln oder Schlüsselgruppen vorhanden sind, empfiehlt Dell die Umbenennung der Duplikate der Schlüssel und Schlüsselgruppen in EKM 2.X, bevor Sie diese in EKM 3.0 zusammenführen. Beziehen Sie sich auf das EKM 2.X Benutzerhandbuch, um weitere Informationen zu erhalten. Wenn die Duplikate der Schlüssel oder Schlüsselgruppen veraltet sind, können Sie diese in EKM 2.X löschen. Das Löschen eines Schlüssels entspricht jedoch dem Löschen aller Daten, die mit diesem Schlüssel geschützt werden, da die Daten nicht mehr zugänglich sind. Aus Sicherheitsgründen besteht keine Möglichkeit, gelöschte Schlüssel wiederherzustellen.

Wenn Duplikate von Geräten vorhanden sind, müssen Sie ein Gerät in EKM 2.X löschen.

Wenn Sie beim Durchführen des Zusammenlegungsverfahrens den folgenden Fehler erhalten, dann löschen Sie das entsprechende Element basierend auf der Fehlermeldung.

```
Duplicate <item> = <item> Migration failed. Please refer to the debug file for
more information. (Doppelt vorhanden <Element> = <Element>Migration
fehlgeschlagen. Bitte beziehen Sie sich für weitere Informationen auf die
Debugdatei.)
```

Beziehen Sie sich auf den entsprechenden Abschnitt:

- Löschen des ekmcert-Zertifikats
- Löschen eines spezifischen Schlüssels
- Löschen eines Gerätes

Löschen des ekmcert-Zertifikats

Jede EKM 2.X-Installation verfügt über ein **ekmcert**-Zertifikat. Wenn Sie mehr als ein EKM 2.X in EKM 3.0 zusammenführen oder migirieren, müssen Sie das **ekmcert-**Zertifikat in EKM 3.0 löschen, bevor Sie versuchen, ein neues EKM 2.X zusammenzuführen.

Da **ekmcert** ein Zertifikat ist und kein Schlüssel, ist es nicht Teil jeglicher Schlüsselgruppen auf dem EKM 3.0 Server. Daher ist bei einer Zusammenführung einer EKM 2.X Version in EKM 3.0 bei anschließendem Entfernen der EKM 2.X Schlüsselgruppen aus EKM 3.0 das **ekmcert** Zertifikat der Zusammenführung nach wie vor auf dem EKM 3.0 Server vorhanden, und ist möglicherweise immer noch vorhanden, wenn Sie mit einer früheren Sicherung wiederherstellen. Da das Zusammenführungstool versucht, das **ekmcert-**Zertifikat erneut hinzuzufügen, schlägt die Zusammenführung fehl.

Sie müssen das **ekmcert-Zertifikat** aus dem EKM 3.0 Server entfernen, wenn eine der folgenden Situationen besteht:

- Sie haben während des EKM 3.0-Installationsverfahrens ein EKM 2.X auf EKM 3.0 migiriert
- Es ist nicht das erste Mal, das Sie EKM 2.X in EKM 3.0 zusammenführen
- Sie müssen eine zuvor zusammengeführte oder migrierte EKM 2.X Version löschen
- Sie erhalten den folgenden Fehler, wenn Sie eine Zusammenführung versuchen. Dieser Fehler weist darauf hihn, dass das **ekmcert-**Zertifikat in EKM 3.0 bereits vorhanden ist:

  ```
  Duplicate Key Alias = ekmcert Migration failed. Please refer to the debug file for more information. (Doppelt vorhandener Schlüsselalias = ekmcert-Migration fehlgeschlagen. Bitte beziehen Sie sich für weitere Informationen auf die Debugdatei.)
  ```

Beziehen Sie sich für das Löschen des **ekmcert-**Zertifikats auf Löschen des ekmcert-Zertifikats.

Löschen des ekmcert-Zertifikats

Führen Sie die folgenden Schritte durch, um zu prüfen, ob das **ekmcert**-Zertifikat auf EKM 3.0 vorhanden ist und es zu löschen:

1. Melden Sie sich am EKM 3.0 Portal an. Beziehen Sie sich auf Anmeldung am Encryption Key Manager 3.0 Portal.

   Es wird der Bildschirm **Willkommen bei Dell Encryption Key Manager angezeigt**.

2. Navigieren Sie im Navigationsfensterbereich zu **Dell Encryption Key Manager → Erweiterte Konfiguration → Server-Zertifikate**.

   Es wird der Bildschirm **Verwaltung von Server-Zertifikaten** angezeigt.

3. Überprüfen Sie auf dem Bildschirm **Verwaltung von Server-Zertifikaten,** ob das **ekmcert-**Zertifikat aufgeführt wird und sich momentan nicht in Verwendung befindet.

   Wenn das **ekmcert** Zertifikat sich momentan nicht in Verwendung befindet, dann gehen Sie weiter zum nächsten Schritt. Wenn sich das **ekmcert** Zertifikat momentan in Verwendung befindet, dann führen Sie die folgenden Schritte durch:

   a) Wählen Sie das **ekmcert**-Zertifikat aus.
   b) Klicken Sie auf **Bearbeiten**.
   c) Heben Sie die Aktivierung des Kontrollkästchens **Aktuelles Zertifikat befindet sich in Verwendung** auf.
   d) Klicken Sie auf **Zertifikat bearbeiten**.

      Es wird der Bildschirm **Verwaltung von Server-Zertifikaten** angezeigt. Das Zertifikat wird als nicht in Verwendung befindlich angezeigt.

4. Wählen Sie das **ekmcert**-Zertifikat erneut aus.

5. Klicken Sie oben in der Tabelle auf **Löschen**.

   Ein Bestätigungsfenster wird angezeigt.

6. Klicken Sie auf **OK**, um das Zertifikat zu löschen.

   Das Zertifikat wird aus der Liste entfernt.

Löschen eines spezifischen Schlüssels

Dieses Kapitel beschreibt das Löschen eines einzelnen Schlüssels. Zu einem Gerät zugehörige Schlüssel können nicht gelöscht werden.

VORSICHT: Das Löschen einer Schlüsselgruppe löscht alle Schlüssel in dieser Schlüsselgruppe. Das Löschen eines Schlüssels entspricht dem Löschen aller Daten, die durch diesen Schlüssel geschützt wurden, da die Daten nicht länger zugänglich sind. Es gibt aus Sicherheitsgründen keine Möglichkeit, gelöschte Schlüssel wiederherzustellen.

ANMERKUNG: Wenn Sie bei Durchführen einer Zusammenführung von EKM 2.X auf EKM 3.0 eine Fehlermeldung erhalten haben, die besagt, dass Sie ein Schlüsselduplikat haben, empfiehlt Dell, dass Sie den doppelt vorhandenen Schlüssel in EKM 2.X umbenennen. Beziehen Sie sich auf das EKM 2.X Benutzerhandbuch, um weitere Informationen zu erhalten.

1. Melden Sie sich am EKM 3.0 Portal an. Beziehen Sie sich auf Anmeldung am Encryption Key Manager 3.0 Portal.
   Es wird der Bildschirm **Willkommen bei Dell Encryption Key Manager** angezeigt.
2. Navigieren Sie im Navigationsfensterbereich zu **Dell Encryption Key Manager → Schlüssel- und Geräteverwaltung**.
   Es wird der Bildschirm **Schlüssel- und Geräteverwaltung** angezeigt.
3. Wählen Sie im Dropdown-Menü **Schlüssel und Geräte verwalten LTO** aus und klicken Sie auf **Start**.
   Es wird der Bildschirm **Schlüssel- und Geräteverwaltung** angezeigt.
4. Wählen Sie im Dropdown-Menü oben in der Tabelle **Schlüssel, Schlüsselgruppenmitgliedschaft und Laufwerke anzeigen** aus.
   Die Schlüssel werden in der Tabelle angezeigt.
5. Wählen Sie den Schlüssel aus, den Sie löschen wollen, um ihn zu markieren und klicken Sie auf „Löschen".
6. Klicken Sie oben in der Tabelle auf **Löschen**.
   Es wird ein Popup-Bestätigungsfenster angezeigt.
7. Wenn Sie sich sicher sind, dass Sie den gewählten Schlüssel löschen wollen, dann klicken Sie auf **OK**.
   Der Schlüssel wird gelöscht.

Löschen eines Gerätes

Dieses Kapitel beschreibt das Löschen eines Gerätes. Ein Gerät ist ein in der Band-Library installiertes, einzelnes Llaufwerk. Die Seriennummer wird auf der rechten Seite der Band-Library angezeigt.

ANMERKUNG: Wenn Sie bei Durchführen einer Zusammenführung von EKM 2.X auf EKM 3.0 eine Fehlermeldung erhalten haben, die besagt, dass Sie ein Geräteduplikat haben, empfiehlt Dell, dass Sie das doppelt vorhandene Gerät in EKM 2.X löschen. Beziehen Sie sich auf das EKM 2.X Benutzerhandbuch, um weitere Informationen zu erhalten.

Führen Sie die folgenden Schritte durch, um ein Gerät aus EKM 3.0 zu löschen.

1. Melden Sie sich am EKM 3.0 Portal an. Beziehen Sie sich auf Anmeldung am Encryption Key Manager 3.0 Portal.
   Es wird der Bildschirm **Willkommen bei Dell Encryption Key Manager** angezeigt.
2. Navigieren Sie im Navigationsfensterbereich zu **Dell Encryption Key Manager → Schlüssel- und Geräteverwaltung**.
   Es wird der Bildschirm **Schlüssel- und Geräteverwaltung** angezeigt.
3. Wählen Sie im Dropdown-Menü **Schlüssel und Geräte verwalten** die Gerätegruppe aus, die das Gerät enthält, das Sie löschen wollen.
4. Klicken Sie auf **Start**.
   Es werden die zur Gerätegruppe zugehörigen Geräte aufgeführt.
5. Klicken Sie das Gerät an, das Sie löschen wollen, um es zu markieren.

6. Klicken Sie oben in der Tabelle auf **Löschen**.

   Es wird ein Popup-Bestätigungsfenster angezeigt.

7. Klicken Sie im Popup-Fenster auf **OK**.

   Das Gerät wird gelöscht.

Überprüfung der Entfernung der EKM 2.X Keystore-Library aus EKM 3.0

Dieses Verfahren ist optional. Dieses Kapitel beschreibt, wie Sie überprüfen, ob alle EKM 2.X Keystore-Einträge (das **ekmcert**-Tertifikat) und die Schlüssel im EKM 2.X Keystore) vom EKM 3.0-Server entfernt wurden. Führen Sie dazu die folgenden Schritte durch:

1. Navigieren Sie in einer Eingabeaufforderung oder Terminalsitzung auf dem EKM 3.0-Server zu dem Ordner, den Sie während des EKM 2.X auf EKM 3.0 Zusammenführungsverfahrens erstellt haben (zum Beispiel, **C:\EKM_Files** in Windows, oder **/opt/EKM_Files** in Linux).
2. Stellen Sie sicher, dass das Java SDK-Tool **keytool** in Befehlszeilenpfad vorhanden ist.
3. Führen Sie die Inhalte des EKM 2.X Keystores aus, indem Sie den folgenden Befehl geben:

   ```
   keytool -list -keystore <EKM_2.X_Keystorename> -storetype JCEKS
   ```

   wobei <*EKM_ 2.X_ Keystorename*> der Name des EKM 2.X-Keystores ist, den Sie importieren.

   Zum Beispiel:

   keytool -list -keystore *EKMKeys.jck* -storetype JCEKS

   Das System fordert Sie zur Eingabe eines Kennworts auf.

4. Geben Sie das EKM 2.X Keystore-Kennwort ein und drücken Sie die **Eingabetaste.**.

   Es werden der EKM 2.X Keystore-Typ, das **ekmcert**-Zertifikat, der Keystore-Anbieter und die Schlüssel im EKM 2.X Keystore angezeigt. Sie werden die Liste der Schlüssel für den Vergleich mit dem EKM 3.0 Keystore verwenden, um zu überprüfen, dass diese Schlüssel im EKM 3.0 Keystore nicht enthalten sind.

ANMERKUNG: Lassen Sie die Befehlszeile offen. In einem späteren Schritt werden Sie nach diesen Schlüsseln und/oder dem **ekmcert-Zertifikat** im EKM 3.0 Keystore suchen, um zu überprüfen, ob diese aus EKM 3.0 entfernt wurden.

5. Starten Sie den EKM 3.0-Server, indem Sie den **startserver**-Befehl verwenden. Beziehen Sie sich auf Starten und Stoppen des EKM 3.0 Servers in Windows oder Starten und Stoppen des EKM 3.0 Servers in Linux.
6. *Navigieren Sie in einer Windows-Befehlszeile zu***<*Stammverzeichnis*>:\Dell\EKM\bin**. *Navigieren Sie in Linux zu* **/opt/dell/ekm/bin**.
7. Melden Sie sich am WebSphere-Server unter Verwendung des Befehls **wsadmin** an. Beziehen Sie sich auf Anmeldung am WebSphere-Server.
8. Geben Sie in der **wsadmin**-Eingabeaufforderung unter Verwendung des zuvor bezogenen Schlüsselalias einen der folgenden Befehle ein, um einen spezifischen Schlüssel oder ein Zertifikat auf dem EKM 3.0-Server aufzuführen:

   Für Schlüssel:

   ```
   print AdminTask.tklmKeyList('[-alias <key alias>]')
   ```

   Für das **ekmcert**-Zertifikat:

   ```
   print AdminTask.tklmKeyList('[-alias ekmcert]')
   ```

ANMERKUNG: Sie haben die Schlüsselaliase in einem vorhergehenden Schritt erhalten. In Windows können Sie die Aliase unter Verwendung der Symbolleiste des Fensters der Befehlszeile kopieren.

ANMERKUNG: Wenn Sie die Schlüsselaliase visuell vergleichen wollen, können Sie alle Schlüssel auf dem EKM 3.0-Server aufführen, indem Sie den folgenden Befehl geben:

```
print AdminTask.tklmKeyList('[-alias ekmcert]')
```

9. Drücken Sie die **Eingabetaste.**

   Der Befehl wird ausgeführt.

Wenn das Schlüsselduplikat nicht in EKM 3.0 vorhanden ist, wird der folgende Text angezeigt:

```
Found 0 keys (0 Schlüssel gefunden).
```

Wenn der Schlüssel, bzw. das Zertifikat in EKM 3.0 vorhanden ist, werden die UUID und der Schlüssel bzw. das Zertifikat angezeigt.

Wenn der Schlüssel, bzw. das Zertifikat in EKM 3.0 vorhanden ist, dann löschen Sie den Schlüssel oder das Zertifikat aus EKM 3.0. Beziehen Sie sich auf Löschen eines spezifischen Schlüssels.

Wiederholen Sie diesen Schritt für jedes Schlüsselduplikat, das zuvor aufgeführt wurde.

7

Deinstallation von EKM 3.0

Dieses Kapitel beschreibt die Deinstallation von EKM 3.0 unter Windows und Linux.

VORSICHT: Durch die Deinstallation von EKM 3.0 werden alle verschlüsselten Daten unlesbar gemacht, die durch die Dell LME (Library-Managed Rncryption)-Verschlüsselung in die PowerVault Band-Library geschrieben wurden. Stellen Sie sicher, dass alle wichtigen Daten wiederhergestellt wurden, bevor Sie EKM 3.0 deinstallieren. Wenn die Möglichkeit besteht, dass Sie zukünftig EKM 3.0 erneut installieren, dann erstellen Sie vor der Deinstallation von EKM 3.0 eine Sicherung. Kopieren Sie das EKM 3.0 Sicherungs- und Installationsprofil (wenn Sie ein Installationsprofil gespeichert haben) auf ein externes Laufwerk, bevor Sie EKM 3.0 deinstallieren. Verwenden Sie diese Sicherungsdatei, um den Wiederherstellungsvorgang durchzuführen, wenn Sie EKM 3.0 erneut installieren. Beziehen Sie sich auf Durchführen von Sicherungen und Wiederherstellen aus einer Sicherung.

ANMERKUNG: Der Deinstallationsvorgang nimmt etwa 35 Minuten in Anspruch. Schalten Sie das System nicht aus, bevor der Deinstallationsvorgang abgeschlossen wurde.

ANMERKUNG: Die Deinstallation von EKM 3.0 deinstalliert auch WebSphere und DB2. Wenn Sie DB2 für andere Anwendungen verwenden, empfiehlt Dell, dass Sie den EKM 3.0-Dienst nicht deinstallieren. Es wird empfohlen, stattdessen den EKM 3.0-Dienst zu stoppen. Beziehen Sie sich auf Starten und Stoppen des EKM 3.0 Servers in Windows oder Starten und Stoppen des EKM 3.0 Servers in Linux.

ANMERKUNG: Wenn Sie einen primären/sekundären Server eingerichtet haben, müssen Sie den Deinstallationsvorgang außerdem auf dem sekundären EKM 3.0-Server durchführen.

ANMERKUNG: Beziehen Sie sich auf Erneutes Installieren von EKM 3.0.

Deinstallation von EKM 3.0 unter Windows

Dieses Verfahren verwendet das EKM 3.0 Deinstallationsprogramm für Windows.

ANMERKUNG: Der Deinstallationsvorgang nimmt etwa 35 Minuten in Anspruch. Schalten Sie das System nicht aus, bevor der Deinstallationsvorgang abgeschlossen wurde.

1. Öffnen Sie in Windows 2008-Versionen die **Systemsteuerung** und navigieren Sie zu **Programme und Funktionen**.
   Öffnen Sie in Windows Server 2003 R2 mit Service Pack 2 die **Systemsteuerung** und navigieren Sie zu **Software hinzufügen oder entfernen**.
2. Klicken Sie mit der rechten Maustaste auf **EKM 3.0** und wählen Sie **Deinstallieren**.
3. Folgen Sie den Anweisungen auf dem Bildschirm.
   Wenn die Deinstallation abgeschlossen wurde, wird das Fenster **Deinstallation abgeschlossen** angezeigt.
4. Klicken Sie im Fenster **Deinstallation abgeschlossen** auf **Vollständig**.
   Es wird ein Dialogfeld angezeigt, dass das System neu gestartet wird.
5. Klicken Sie im Dialogfeld auf **Vollständig**. (Wenn Sie nicht auf **Vollständig** klicken, wird Windows dennoch nach etwa einer Minute neu gestartet.)

ANMERKUNG: Starten Sie den computer manuell neu, wenn Windows nicht neu gestartet wird.

ANMERKUNG: Wenn während des Deinstallationsvorgangs Fehler auftreten, können Sie das Hauptinstallationsprotokoll im Benutzer-Startverzeichnis unter **<*Stammverzeichnis*>:\Benutzer\Administrator** anzeigen lassen. Die Hauptinstallationsdatei ist **IA-TIPxxx**. Scrollen Sie in der Hauptinstallationsdatei ganz nach unten, um zu bestimmen, wo der Vorgang gestoppt wurde oder der letzte Fehler aufgetreten ist. Sie können die Protokolldateien auch in **<*Stammverzeichnis*>:\tklmv2properties** anzeigen lassen, um weitere Einzelheiten zu erfahren.

ANMERKUNG: Wenn Sie EKM 3.0 erneut installieren und die Installation aufgrund einer unvollständigen Deinstallation fehlschlägt, dann führen Sie die Deinstallation manuell durch. Beziehen Sie sich auf Manuelle Deinstallation von EKM 3.0 in Windows.

Deinstallation von EKM 3.0 in Linux

Dieses Verfahren verwendet das EKM 3.0-Deinstallationsprogramm für Linux.

ANMERKUNG: Der Deinstallationsvorgang nimmt etwa 35 Minuten in Anspruch. Schalten Sie das System nicht aus, bevor der Deinstallationsvorgang abgeschlossen wurde.

1. Öffnen Sie eine Terminalsitzung und navigieren Sie zu **/opt/dell/ekm/Uninstall_EKM**.
2. Führen Sie **EKM-Deinstallation** aus, indem Sie den folgenden Befehl geben:

   ```
   ./Uninstall EKM
   ```

   Es wird ein Popup-Fenster angezeigt.
3. Klicken Sie im Popup-Fenster auf **Ausführen**.

   Das Fenster **EKM-Deinstallation** wird angezeigt.
4. Klicken Sie auf **Deinstallieren**.

   Der Deinstallationsvorgang wird ausgeführt.
5. Wenn die Deinstallation abgeschlossen wurde, wird das Fenster **Deinstallation abgeschlossen** angezeigt. Klicken Sie auf **Fertig**.

   Das System wird neu gestartet.

ANMERKUNG: Wenn Sie EKM 3.0 erneut installieren und die Installation aufgrund einer unvollständigen Deinstallation fehlschlägt, dann führen Sie die Deinstallation manuell durch. Beziehen Sie sich auf Manuelle Deinstallation von EKM 3.0 in Linux.

8

Fehlerbehebung

Dieses Kapitel enthält Informationen zur Fehlerbehebung, häufig gestellte Fragen (FAQ), allgemeine Fehlermeldungen und Support-Kontaktinformationen.

ANMERKUNG: Wenn Ihr Problem in diesem Kapitel nicht behandelt wird, dann beziehen Sie sich auf das TKLM-Fehlerbehebungshandbuch. Lesen Sie den Abschnitt „Dokumentations- und Referenzmaterialien" der Datei **ReadThisFirst.txt** auf dem EKM 3.0 Installationsdatenträger, um Informationen über den Zugriff auf die TKLM-Dokumentation zu erhalten.

Kontaktaufnahme mit Dell

ANMERKUNG: Wenn Sie nicht über eine aktive Internetverbindung verfügen, können Sie Kontaktinformationen auch auf Ihrer Auftragsbestätigung, dem Lieferschein, der Rechnung oder im Dell-Produktkatalog finden.

Dell stellt verschiedene online-basierte und telefonische Support- und Serviceoptionen bereit. Da die Verfügbarkeit dieser Optionen je nach Land und Produkt variiert, stehen einige Services möglicherweise in Ihrer Region nicht zur Verfügung. So erreichen Sie den Vertrieb, den technischen Support und den Kundendienst von Dell:

1. Besuchen Sie **support.dell.com**.
2. Wählen Sie Ihre Supportkategorie.
3. Wenn Sie kein US-Kunde sind, wählen Sie am Ende der Seite ihren Ländercode aus oder wählen Sie **All** (Alle), um für weitere Auswahlmöglichkeiten.
4. Klicken Sie je nach Bedarf auf den entsprechenden Service- oder Support-Link.

Überprüfungen der Systemvoraussetzungen

EKM 3.0 führt vor der Installation Überprüfungen der Systemvoraussetzungen durch. Wenn Sie nach dem **Endbenutzer-Lizenzvereinbarung**-Bildschirm eine Fehlermeldung erhalten, dann folgen Sie den Anweisungen in der Fehlermeldung. Beziehen Sie sich für die häufigsten Fehler auf die untenstehenden Themen, um Anweisungen zu erhalten.

Minimale Systemanforderungen nicht erfüllt

Wenn Sie einen **Minimale Systemanforderungen nicht erfüllt-Fehler** erhalten, dann klicken Sie auf **Abbrechen und Beenden** und bestätigen Sie, dass Ihr System die Anforderungen erfüllt. Beziehen Sie sich auf Hardware- und Softwareanforderungen, um die Systemanforderungen zu erhalten.

Benutzer ist auf diesem System kein Administrator

Sie müssen ein Root-Benutzer auf Linux, bzw. ein Administrator auf Windows sein, um EKM 3.0 installieren zu können.

SELinux muss deaktiviert sein

Wenn SELinux installiert und aktiv ist, dann deaktivieren Sie SELinux, bevor Sie die Installation starten.

Führen Sie zum Deaktivieren von SELinux in RHEL5 die folgenden Schritte durch:

1. Navigieren Sie von der oberen Symbolleiste aus zu **System → Administration Sicherheitsstufe und Firewall.**
   Es wird das Fenster **Sicherheitsstufenkonfiguration** angezeigt.
2. Klicken Sie auf die Registerkarte **SELinux**. Klicken Sie im Feld **SELinux Einstellung** auf die Pfeile und wählen Sie **Deaktiviert** aus.
3. Klicken Sie auf **Übernehmen**.
4. Klicken Sie auf **OK**.
5. Starten Sie das System neu, um die Änderungen in Kraft zu setzen.

Führen Sie zum Deaktivieren von SELinux in RHEL4 die folgenden Schritte durch:

1. Navigieren Sie zu **Anwendungen Systemeinstellungen → Sicherheitsstufe** .
   Es wird ein Popup-Fenster angezeigt.
2. Wählen Sie im Popup-Fenster die Registerkarte **SELinux** aus.
3. Wählen Sie im Dropdown-Menü **Deaktivieren** aus.
4. Starten Sie das System neu.

compat-libstdc++ Not Installed (compat-libstdc++ Nicht installiert)

Wenn eine „compat-libstdc++ Not Installed"-Fehlermeldung angezeigt wird, dann beziehen Sie sich auf Installieren der compat-libstdc++ Library.

Minimum Shared Memory Limits Requirements Failed (Mindestanforderungen für Shared Memory-Grenzwerte nicht erfüllt)

Bei der Installation von EKM 3.0 auf Linux wird der folgende Fehler angezeigt:

```
Das System hat die für die Installation erforderlichen Mindestanforderungen für
die Shared Memory-Grenzwerte nicht erfüllt. Stellen Sie sicher, dass Ihr System
die Mindestanforderungen für die Shared Memory-Grenzwerte erfüllt, bevor Sie
versuchen, diese Installation durchzuführen.
```

Führen Sie zur Behebung dieses Problems die folgenden Schritte durch:

1. Öfnnen Sie eine Terminalsitzung und geben Sie den folgenden Befehl, um den gemeinsamen Speicher (Shared Memory) auf die erforderliche Größe zu erhöhen und ihn beständig zu machen:

   ```
   echo "kernel.msgmni = 1024" >> /etc/sysctl.conf echo "kernel.msgmax =
   65536" >> /etc/sysctl.conf echo "kernel.msgmnb = 65536" >> /etc/sysctl.conf
   ```

```
echo "kernel.sem = 250 256000 32 1024" >> /etc/sysctl.conf echo
"kernel.shmmax = 1268435456" >> /etc/sysctl.conf
```

ANMERKUNG: Dies sind die für die Installation von EKM 3.0 auf Linux mindestens erforderlichen Werte. EKM 3.0 benötigt möglicherweise für eine erfolgreiche Installation mehr gemeinsamen Speicher (kernel.shmmax). Wenn die Installation fehlschlägt, dann deinstallieren Sie EKM 3.0, erhöhen Sie kernel.shmmax um etwa 25% und installieren Sie EKM 3.0 neu. Beziehen Sie sich für die Deinstallation von EKM 3.0 auf Deinstallation von EKM 3.0.

2. Geben Sie den folgenden Befehl, sodass das System die neue Größe des gemeinsamen Speichers sofort nutzt (anderenfalls müssen Sie neu starten):

```
sysctl -p
```

DB2 User Already Exists as Regular User (DB2-Benutzer bereits als regulärer Benutzer vorhanden)

Der für das Feld **DB2 Benutzername** bereitgestellte Benutzernamen ist bereits als Benutzer auf dem System vorhanden. Wählen Sie einen anderen Benutzernamen.

Existing TKLM or EKM 3.0 on the Same System (Vorhandener TKLM oder EKM 3.0 auf dem gleichen System)

TKLM oder EKM 3.0 ist bereits installiert. Deinstallieren Sie die vorhandene Instanz, oder installieren Sie EKM 3.0 auf einem anderen System.

Existing DB2 on the Same System (Vorhandenes DB2 auf dem gleichen System)

DB2 ist bereits installiert. Deinstallieren Sie DB2 oder installieren Sie EKM 3.0 auf einem anderen System.

ksh Not Installed (ksh nicht installiert)

Das EKM 3.0-Installationsprogramm benötigt **ksh**. Installieren Sie **ksh** und installieren Sie anschließend EKM 3.0. Beziehen Sie sich auf die Dokumentation Ihres Betriebssystems.

Hostname has Special Characters (Sonderzeichen im Hostnamen enthalten)

Der Hostname des Computersystems, auf dem Sie EKM 3.0 installieren darf keine Leerzeichen oder Sonderzeichen enthalten, wie z.B. Bindestriche (-) oder Unterstriche (_). EKM 3.0 unterstützt im Hostnamen ausschließlich alphanumerische Zeichen.

Domain Name (Domänenname)

Der Domänenname des Computersystems, auf dem Sie EKM 3.0 installieren darf keine Leerzeichen oder Sonderzeichen enthalten, wie z.B. Bindestriche (-) oder Unterstriche (_). EKM 3.0 unterstützt ausschließlich alphanumerische Zeichen im Domänennamen.

Invalid /etc/hosts file

Die Datei **/etc/hosts** muss einen gültigen Eintrag für die Loopback-IPv4-Adresse enthalten. Der Eintrag muss das folgende Format haben:

<Loopback-IPv4-Adresse><Leertaste><vollständig qualifizierter Hostname><Leertaste><kurzer *Hostname>*

Wobei *<Leertaste>* für ein Leerzeichen steht.

Fehlercodes

Beziehen Sie sich für den Zugang zu einer Liste mit Fehlercodes und deren Beschreibungen auf den Abschnitt „Dokumentation und Referenzmaterialien“ der Datei **ReadThisFirst.txt** auf dem EKM 3.0 Installationsdatenträger.

Windows Referenzdateien

Sie können die folgenden Protokolldateien und Fehlerdateien verwenden, um Probleme mit der EKM 3.0-Installation auf Windows zu beheben:

- **C:\tklm_install.stderr** (Standard-Fehlerprotokolldatei)
- **C:\tklmV2properties*.log** (DB2 Installationsprotokolldateien)
- **C:\Users\Administrator\IA-TIPInstall-00.txt** (EKM 3.0 Installationsprotokolldatei)

ANMERKUNG: Dieser Pfad gilt für Windows Server 2008-Versionen. Für Windows Server 2003 R2 mit Service Pack 2 befindet sich die EKM 3.0 Installationsprotokolldatei in **C:\Dokumente und Einstellungen\Administrator\IA-TIPInstall-00.txt**.

- **C:\Dell\EKM\products\tklm\logs\audit\tklm_audit.txt** (Protokolldatei). (Diese Datei kann über Behebung von Installationsproblemen hinaus auch zur Behebung von Problemen mit der Nutzung verwendet werden.)

ANMERKUNG: Der obige Pfad geht davon aus, das C: das Stammlaufwerk ist. Ersetzen Sie **C: mit dem Buchstaben Ihres Stammlaufwerks**.

Linux-Referenzdateien

Sie können die folgenden Protokolldateien und Fehlerdateien verwenden, um Probleme mit der EKM 3.0-Installation auf Linux zu beheben:

- **/root/IA-TipInstall_*.log**
- **/tklm_install.stderr** (Standard-Fehlerprotokolldatei)
- **/tklmV2properties/*.log**
- **/opt/dell/ekm/products/tklm/logs/audit/tklm_audit.log**

Manuelle Deinstallation von EKM 3.0

Verwenden Sie bei der Deinstallation von EKM 3.0 zuerst das automatisierte Deinstallationsverfahren. Beziehen Sie sich auf Deinstallation von EKM 3.0. Wenn der automatisierte Deinstallationsvorgang fehlschlägt, dann deinstallieren Sie EKM 3.0 manuell.

Manuelle Deinstallation von EKM 3.0 in Windows

Wenn Sie EKM 3.0 neu installieren und die Installation aufgrund einer unvollständigen Deinstallation fehlschlägt, dann führen Sie die Deinstallation manuell durch. Wenn ein Objekt bereits deinstalliert wurde, dann überspringen Sie diesen Schritt.

ANMERKUNG: Wenn Sie die Option haben, das Betriebssystem auf Ihrem Server neu zu installieren, empfiehlt Dell, dass Sie das Betriebssystem neu installieren und anschließend EKM 3.0 installieren.

ANMERKUNG: Die Pfade in diesem Verfahren sind für Windows Server 2008 Versionen gedacht. Navigieren Sie gegebenenfalls für Windows Server 2003 R2 mit Service Pack 2 zu **Start** → **Systemsteuerung** → **Programme hinzufügen oder entfernen** .

1. Navigieren Sie zu **Start** → **Systemsteuerung** → **Programme (oder Programme und Funktionen)** → **Programm deinstallieren** . Deinstallieren Sie IBM DB2 (**DB2 Workgroup Server Edition - DB2TKLMV2**).
2. Navigieren Sie zu **Start** → **Systemsteuerung** → **Programme (oder Programme und Funktionen)** → **Programm deinstallieren**.
3. Klicken Sie auf **EKM**.
4. Klicken Sie auf **Deinstallieren/Ändern**.

   Es wird der Assistent für die EKM 3.0-Deinstallation angezeigt.
5. Befolgen Sie des Anweisungen des Deinstallationsassistenten.

   Nach der Deinstallation von EKM 3.0 wird das System automatisch neu gestartet.
6. Navigieren Sie zu **Start** → **Systemsteuerung** → **Programme** → **Programm deinstallieren**. Deinstallieren Sie **IBM Update Installer for WebSphere software V7.0**.
7. Führen Sie das Windows-Registrierungseditorprogramm aus (Regedit). Navigieren Sie zu **HKEY_CURRENT_USER** → **Software** → **IBM** → **DB2** → **InstalledCopies**. Löschen Sie den Ordner **DB2TLKMV2**.

VORSICHT: Gehen Sie beim Ändern der Registrierung mit besonderer Sorgfalt vor. Wenn Sie eine falsche Änderung vornehmen, kann das System instabil werden.

8. Navigieren Sie in Windows Explorer zu **<*Stammverzeichnis*>:\Dell**, falls vorhanden (zum Beispiel **C:\Dell**). Löschen Sie den Ordner **EKM** (falls vorhanden) und alle seine Unterordner (**<*Stamverzeichnis*>:\Dell\EKM**).
9. Löschen Sie auf dem Stammlaufwerk (zum Beispiel **C:**) den Ordner **tklmV2properties** (**<*Stammverzeichnis*>:\tklmV2properties**).
10. Löschen Sie auf dem Stammlaufwerk den Ordner **tklmdbarchive**. (**<*Stammverzeichnis*>:\tklmdbarchive**).
11. Löschen Sie auf dem Stammlaufwerk den Ordner mit dem gleichen Namen wie der dB2-Benutzername.
12. Löschen Sie auf dem Stammlaufwerk die Datei **tklm_install.stderr file** (**<*Stammverzeichnis*>:\tklm_install.stderr**).
13. Navigieren Sie in Windows Explorer zu **<*Stammverzeichnis*>:\Programme (x86)\dell**. Löschen Sie das DB2-Installationsverzeichnis(**<*Stammverzeichnis*>:\Programme (x86)\dell\db2dkm**).

ANMERKUNG: Ersetzen Sie in diesem Schritt und den folgenden drei Schritten „Programme (x86)" mit „Programme", wenn es sich bei Ihrem Betriebssystem um ein 32-Bit Betriebssystem handelt.

14. Navigieren Sie in Windows Explorer zu **<*Stammverzeichnis*>:*Programme* (x86)\ibm**. Löschen Sie den Ordner **Common** (**<*Stammverzeichnis*>:*Programme* (x86)\ibm\Common**).

15. Navigieren Sie in Windows Explorer zu **<*Stammverzeichnis*>:*Programme* (x86)\ibm**. Löschen Sie den Ordner **gsk8** (**<*Stammverzeichnis*>:*Programme* (x86)\ibm\gsk8**).
16. Navigieren Sie zu **Start** → **Verwaltung** → **Computerverwaltung** . Navigieren Sie im linken Fensterbereich zu **Lokale Benutzer und Gruppen** → **Benutzer** . Löschen Sie im rechten Fensterbereich das/die DB2 Administratorkonto/-konten.
17. Navigieren Sie zu **Start** → **Verwaltung** → **Computerverwaltung** . Navigieren Sie im linken Fensterbereich zu **Lokale Benutzer und Gruppen** → **Gruppen** . Löschen Sie im rechten Fensterbereich die DB2 Administratorgruppen (**DB2ADMINS** und **DB2USERS**).
18. Navigieren Sie in Windows Explorer zu **<*Stammverzeichnis*>:\Benutzer**. Löschen Sie den Ordner mit dem gleichen Namen wie der DB2 Benutzername.
19. Navigieren Sie in Windows Explorer zu **<*Stammverzeichnis*>:\Benutzer\Administrator**. Löschen Sie die Textdatei **IA-TIPInstall-xx log**.
20. Stoppen und löschen Sie alle folgenden installierten EKM 3.0 Windows-Dienste. Geben Sie dazu in einer Eingabeaufforderung auf dem Stammlaufwerk (zum Beispiel **C:**) die folgenden Befehle ein. Wenn der Dienst bereits gestoppt wurde, können Sie den Schritt „Stoppen“ überspringen.

ANMERKUNG: Falls gewünscht, können Sie die Dienste vom Programm „Windows-Dienste“ aus löschen

```
sc stop "DBTKLM20" sc delete "DBTKLM20" sc stop "<DB2 Benutzername>" sc
delete "<DB2 Benutzername>" sc stop "DB2GOVERNOR_DB2TKLMV2" sc delete
"DB2GOVERNOR_DB2TKLMV2" sc stop "DB2LICD_DB2TKLMV2" sc delete
"DB2LICD_DB2TKLMV2" sc stop "DB2MGMTSVC_DB2TKLMV2" sc delete
"DB2MGMTSVC_DB2TKLMV2" sc stop "DB2REMOTECMD_DB2TKLMV2" sc delete
"DB2REMOTECMD_DB2TKLMV2" sc stop "DB2DAS00" sc delete "DB2DAS00"
```

ANMERKUNG: Der folgende Dienst wird im Programm „Windows-Dienste“ als **Tivoli Integrated Portal - TIPProfile_Port_*<DB2 Portnummer>*** angezeigt.

```
sc stop "IBMWAS61Service - TIPProfile_Port_<DB2 Portnummer>" sc delete
"IBMWAS61Service - TIPProfile_Port_<DB2 Portnummer>"
```

ANMERKUNG: Die Standardeinstellung der DB2 Portnummer ist 16310.

21. Geben Sie in einer Eingabeaufforderung auf dem Stammlaufwerk (zum Beispiel **C:)** die folgenden Befehle ein.

```
reg delete HKEY_LOCAL_MACHINE\software\classes\installer\Products
\907E425044C581845A83FCBED0CD5771 /f reg delete HKEY_LOCAL_MACHINE\software
\classes\installer\Features\907E425044C581845A83FCBED0CD5771 /f
```

22. Starten Sie das System neu.
23. Wenn Sie EKM 3.0 neu installieren wollen, dann beziehen Sie sich auf Durchführung des EKM 3.0 Installationsverfahrens.

Manuelle Deinstallation von EKM 3.0 in Linux

Wenn Sie EKM 3.0 neu installieren und die Installation aufgrund einer unvollständigen Deinstallation fehlschlägt, dann führen Sie die Deinstallation manuell durch. Wenn irgendein Element bereits deinstalliert wurde, dann überspringen Sie diesen Schritt.

ANMERKUNG: Wenn Ihr Server die Option zur Neuinstallation des Betriebssystems hat, empfiehlt Dell, dass Sie das Betriebssystem neu installieren und anschließend EKM 3.0 installieren.

Ersetzen Sie in folgendem Verfahren die folgenden Variablen (<*variable*>) mit Ihren Installationspfaden oder Variablennamen.

- <*DB2_INSTALL_DIR*>: Dies ist das Verzeichnis, das Sie für die Datenbankinstallation ausgewählt haben.
- <*DB2_ADMIN*>: Dies ist die DB2 Administrator-ID (z.B. **ekm_dell1**).
- <*DB2_ADMIN_HOME*>: Dies ist das Startverzeichnis der Datenbank (auch als Datenbank-Datenspeicherort bezeichnet).

- *<DB2_DB_NAME>*: Dies ist der Datenbankname.

1. Öffnen Sie eine Terminalsitzung.
2. Entfernen Sie die DB2-Instanz, indem Sie die folgenden Befehle eingeben:

   ```
   cd /opt/dell/ekm/products/tklm/_uninst ./removeDB2Inst.sh
   <DB2_INSTALL_DIR> ./removeDB2Inst.sh <DB2_ADMIN> ./removeDB2Inst.sh
   <DB2_ADMIN_HOME> ./removeDB2Inst.sh <DB2_DB_NAME>
   ```

   Zum Beispiel:

   ```
   ./removeDB2Inst.sh /opt/dell/db2ekm ./removeDB2Inst.sh /ekm_dell1 ./
   removeDB2Inst.sh /home/db2ekm ./removeDB2Inst.sh /db2ekm
   ```

3. Führen Sie die TKLM Deinstallation im Hintergrund aus, indem Sie die folgenden Befehle eingeben:

   ```
   /opt/dell/ekm/_uninst/TIPInstall/uninstall -i silent –f /opt/dell/ekm/
   Uninstall_EKM/dkm_uninstall_response.txt
   ```

4. Entfernen Sie die Protokolldateien, indem Sie die folgenden Befehle eingeben:

   ```
   rm –rf /tklmV2properties cd /opt/dell/ekm/ rm tklm_install.stderr rm IA-
   TIPIn*.log rm EKM_Install*.log
   ```

5. Entfernen Sie die DB2-Benutzer-ID, indem Sie den folgenden Befehl eingeben:

   ```
   userdel -r $DB2_ADMIN$
   ```

   Zum Beispiel:

   ```
   userdel -r ekm_dell1
   ```

6. Entfernen Sie DB2 vom System, indem Sie die folgenden Befehle eingeben:

   ```
   cd /opt/dell/ekm/install ./db2_deinstall -a
   ```

7. Entfernen Sie das für die EKM 2.X Zusammenführung/Migration und die EKM 3.0-Installation verwendete Stammverzeichnis.

   ```
   rm –rf /opt/dell/ekm
   ```

8. Starten Sie den Computer neu.
9. Wenn Sie EKM 3.0 neu installieren wollen, dann beziehen Sie sich auf Durchführung des EKM 3.0 Installationsverfahrens.

Erneutes Installieren von EKM 3.0

Führen Sie die folgenden Schritte durch, um EKM 3.0 neu zu installieren:

1. Deinstallieren Sie EKM 3.0 unter Verwendung des Deinstallationsverfahrens. Beziehen Sie sich auf Deinstallation von EKM 3.0.

ANMERKUNG: Wenn der Computer bei der Deinstallation von EKM 3.0 nicht automatisch neu gestartet wurde, dann starten Sie den Computer neu.

2. Installieren Sie EKM 3.0 unter Verwendung des Installationsverfahrens. Beziehen Sie sich auf Durchführung des EKM 3.0 Installationsverfahrens.

ANMERKUNG: Wenn Sie während der ursprünglichen ELM 3.0-Installation ein Installationsprofil gespeichert haben, können Sie dieses zur Neuinstallation von EKM 3.0 verwenden. Wenn Sie jedoch eine Primär/Sekundärserverkonfiguration verwenden und das Installationsprofil zum sekundären EKM 3.0-Server gehört, dann verwenden Sie dieses nicht zur Neuinstallation von EKM 3.0 auf dem Primärserver.

Häufig gestellte Fragen (FAQs)

Kann ich EKM 3.0 auf einem Betriebssystem installieren, das im Kapitel Hardware- und Softwareanforderungen nicht aufgeführt ist?

Nein. EKM 3.0 unterstützt ausschließlich die in Hardware- und Softwareanforderungen aufgeführten Betriebssysteme, deren Versionen, Editionen, Service-Pack-Stufen und Bit-Stufen

Kann ich Dateien aus dem EKM 3.0-Installationsprogramm auf mein System kopieren und es von meinem lokalen System aus installieren??

Nein. EKM 3.0 unterstützt ausschließlich die Installation vom EKM 3.0-Datenträger aus. Beziehen Sie sich auf EKM 3.0-Installation.

Wie gehe ich vor, wenn ich während der EKM 3.0-Installation eine Fehlermeldung erhalte, die besagt, dass die Installation im Hintergrund fehlgeschlagen ist?

Beziehen Sie sich für weitere Informationen auf die Datei **tklm_install.stderr** (Standard-Protokolldatei). *In Windows* befindet sich diese Datei in ***<Stammverzeichnis>***:**tklm_install.stderr**. *In Linux* befindet sie sich in **/tklm_install.stderr**. Wenn in dieser Datei ein Fehlercode aufgeführt wird, dann beziehen Sie sich auf Fehlercodes.

Führen Sie nach Behebung der durch den Fehlercode beschriebenen Fehlersituation eine manuelle Deinstallation durch. Beziehen Sie sich auf EKM 3.0 - Manuelle Deinstallation. Starten Sie das System neu, nachdem Sie EKM 3.0 manuell deinstalliert haben und installieren Sie anschließend EKM 3.0 neu.

Wie gehe ich vor, wenn ich bei der Neuinstallation von EKM 3.0 eine Fehlermeldung erhalte, die besagt, dass die Installation fehlgeschlagen ist?

Führen Sie eine manuelle Deinstallation durch. Beziehen Sie sich auf EKM 3.0 - Manuelle Deinstallation. Starten Sie das System neu, nachdem Sie EKM 3.0 manuell deinstalliert haben und installieren Sie EKM 3.0 anschließend neu.

Wie gehe ich vor, wenn ich während der EKM 3.0-Installation eine Fehlermeldung erhalte, die besagt, dass Windows Server 2003 R2 SP2 nicht installiert wurde?

Beziehen Sie sich für eine Liste der unterstützten Betriebssysteme auf Hardware- und Softwareanforderungen. Starten Sie nach Installation der zweiten Windows Server 2003 R2 CD das System neu, bevor Sie EKM 3.0 installieren.

VORSICHT: Dieser Vorgang überschreibt die Daten auf dem Band-Datenträger. Sobald die Daten überschrieben wurden, sind die Daten des Band-Datenträgers nicht mehr zugänglich.

Wie verwende ich bereits verschlüsselte Datenträger als nichtverschlüsselte Datenträger, oder als verschlüsselte Datenträger mit einem anderen Verschlüsselungscode?

Das erneute Verwenden bereits verschlüsselter Datenträger erfordert die Verwendung einer funktionierenden EKM 3.0-Konfiguration, die die Schlüssel für die erneut zu verwendenden Bänder enthält und einen PowerVault TL2000 oder TL4000.

Auf dem PowerVault ML6000 können Bänder nicht auf diese Weise überschreiben werden. Sie können zu diesem Zweck Bänder von einem ML6000 auf einen TL2000 oder TL4000 migrieren. Sie müssen den TL2000 oder TL4000 anschließend auf einen entsprechenden EKM 3.0 Server verweisen.

Führen Sie die folgenden Schritte durch, um bereits verschlüsselte Datenträger erneut zu verwenden:

1. Stellen Sie sicher, dass der EKM 3.0 Server ausgeführt wird und ordnungsgemäß konfiguriert wurde.
2. Melden Sie sich beim TL2000/TL4000 an der RMU GUI an (Administrator/Service-Anmeldung erforderlich).
3. Navigieren Sie zu **Library konfigurieren**.
4. Navigieren Sie zu **Verschlüsselung**.
5. Ändern Sie die Einstellungen der **Verschlüsselungsrichtlinien** auf **Interne Bezeichnung – Selektive Verschlüsselung**.
6. Senden Sie einen Schreibauftrag (zum Beispiel eine Schnellöschung, reguläre Löschung, oder Sicherung) an den wiederzuverwendenden Datenträger.

Führen Sie die folgenden Schritte durch, um zu überprüfen, dass die Verschlüsselung überschrieben wurde:

1. Melden Sie sich beim TL2000/4000 an der RMU GUI an.

2. Navigieren Sie zu **Library-Überwachung** und anschließend zu **Bestand**.
3. Klicken Sie für das geeignete Magazin auf das Dropdown-Menü.
4. Überprüfen Sie, dass der Abschnitt **Kommentar Nicht verschlüsselt** anzeigt.

Sie können EKM 3.0 nur entfernen oder deinstallieren, nachdem alle gewünschten Datenträger überschrieben wurden. Dell empfiehlt, dass Sie eine Sicherung der wichtigsten Dateien in der EKM 3.0 GUI vornehmen und die Dateien auf einer externen Quelle, wie z.B. einem Wechsellaufwerk sichern. Dadurch kann EKM 3.0 wiederhergestellt werden, wenn weitere Bänder überschrieben werden müssen.

Ich habe Probleme mit einer neuen EKM 3.0-Installation und muss eine Neuinstallation vornehmen. Wie kann ich feststellen, ob der EKM 3.0 jemals Schlüssel bereitgestellt hat?

1. Öffnen Sie eine Eingabeaufforderung und navigieren Sie in das Verzeichnis mit der Protokolldatei.

   In Windows befindet sich das Prüfprotokoll in ***<Stammverzeichnis>*:\Dell\EKM\products\tklm\logs\audit\tklm_audit.txt**.

   In Linux befindet sich das Prüfprotokoll in **/opt/dell/ekm/products/tklm/logs/audit/tklm_audit.log.**
2. Kopieren Sie die aktuelle Prüfprotokolldatei in eine temporäre Datei, sodass sie geöffnet werden kann. Die aktuelle Prüfprotokolldatei ist aktiv und kann nicht geöffnet werden, während sie aktualisiert wird.
3. Öffnen Sie die temporäre Kopie in einem Texteditor (zum Beispiel WordPad). Suchen Sie nach **Drive Serial Number**. Wenn ein Eintrag vorhanden ist, wurde ein Schlüssel bereitgestellt. Wenn der Eintrag **volser** leer ist, ist dies das Ergebnis der Schlüsselpfaddiagnose und Sie sollten die Datei zur Sicherheit nach weiteren mit der Laufwerksseriennummer verbundenen Einträgen durchsuchen.

VORSICHT: Wenn Schlüssel bereitgestellt wurden, müssen Sie die Daten auf den betreffenden Datenträgern entschlüsseln, bevor Sie EKM 3.0 deinstallieren.

Welchen Einfluss hat es auf meine Sicherungsanwendung, wenn ich die Band-Library für LME (Library Managed Encryption) konfiguriere?

Wenn Sie auf der Library LME aktiviert haben und Partitionen mit aktiver Verschlüsselung konfiguriert haben, werden an den/dem Laufwerk(en) in diesen Partitionen Änderungen der Laufwerkseinstellungen vogenommen. Sie müssen die Sicherungsanwendungsdienste nach Konfiguration der Partitionen mit aktiver Verschlüsselung stoppen und starten, um sicherzustellen, dass die Sicherungsanwendung die Verschlüsselungseinstellung(en) des/der Laufwerke erkennt.

ANMERKUNG: Die Bandsicherungsanwendung zeigt die Verschlüsselung nicht als **aktiviert** an, wenn LME verwendet wird. Die Band-Library zeigt die Partitionen als **verschlüsselungsaktiviert** an. LME ist für die Sicherungsanwendung unsichtbar. Die Bandsicherungsanwendung zeigt dieVerschlüsselung nur dann als **aktiviert** an, wenn die Anwendung (zum BeispielSymantec, CommVault, etc.) den/dem Laufwerk(en) die Verschlüsselungscodes bereitstellt.

Wie geht EKM 3.0 mit dem Hinzufügen von neuen Laufwerken oder dem Austausch eines defekten Laufwerks um?

Sie können neue Laufwerke bzw. Ersatzlaufwerke durch die automatische Erkennung, oder manuell zum EKM 3.0 Server hinzufügen. Beziehen Sie sich für das automatische Hinzufügen auf Hinzufügen eines Gerätes zu einer Gerätegruppe.

Dell empfiehlt, dass Sie die automatische Ermittlung verwenden, da die 12-stellige Laufwerksseriennummer (10-stellige Seriennummer plus zwei Nullen zu Anfang) für das manuelle Hinzufügen eingegeben werden muss. Wenn Sie besonderen Wert auf Sicherheit legen, können Sie die automatische Ermittlung einschalten und Testsicherungen oder Schlüsselpfaddiagnosen in der Band-Library ausführen, um die benötigten Laufwerke zur Laufwerkstabelle hinzuzufügen. Anschließend können Sie die automatische Ermittlung ausschalten, um zu verhindern, dass neue Laufwerke Schlüssel erhalten. So lange EKM 3.0 die digitale Signatur authentifizieren kann, die dem Laufwerk ab Werk zugewiesen wurde, akzeptiert EKM 3.0 die Schlüsselanfrage. Die Schlüssel werden im Keystore in Schlüsselgruppen gruppiert und Sie können die Schlüsselgruppen nach Hinzufügen der Laufwerke den neuen Laufwerken, bzw. den Ersatzlaufwerken zuordnen.

ANMERKUNG: Wenn Sie ein Gerät manuell hinzufügen wollen, dann beziehen Sie sich auf die TKLM-Dokumentation. Beziehen Sie sich für Informationen über den Zugang zur TKLM-Dokumentation auf den Abschnitt „Dokumentation und Referenzmaterialien“ der Datei **ReadThisFirst.txt** auf dem EKM 3.0-Installationsdatenträger.

Wie geht EKM 3.0 mit dem Hinzufügen einer neuen Band-Library oder dem Austausch einer defekten Band-Library um?

In der durch die Library verwalteten (LME)-Verschlüsselung ist die Band-Library lediglich ein Proxy. Sie können Band-Libraries hinzufügen oder ersetzen und Schlüssel bereitstellen, solange der EKM 3.0 die digitale Signatur des Laufwerks authentifizieren kann. Die Austausch-Band-Library muss für LME lizenziert sein und für die Verwendung mit dem vorhandenen EKM 3.0 kkonfiguriert werden.

Wie wird die Komprimierung durch die Verschlüsselung beeinflusst und umgekehrt?

Die Daten werden komprimiert, bevor sie verschlüsselt werden, da verschlüsselte Daten im Allgemeinen nicht komprimierbar sind. Daher wirkt sich die Komprimierung nicht auf die Verschlüsselung aus und umgekehrt.

Hat die Verschlüsselung Leistungseinbußen zur Folge?

Möglicherweise hat die Verschlüsselung geringe Leistungseinbußen zur Folge, jedoch sollte sie sich im Sicherungsfenster nicht weiter auswirken.

Wie fordere ich ein Drittanbieter-Zertifikat an und verwende es?

Erstellen Sie in EKM 3.0 eine Zertifikatanforderung. Senden Sie diese Zertifikatanforderung an eine Zertifizierungsstelle (CA). Das durch die Zertifizierungsstelle zurückgegebene Zertifikat kann in EKM 3.0 importiert und für den Schutz von Daten auf Geräten mit aktivierter Verschlüsselung, oder für die SSL-Kommunikation verwendet werden. Lesen Sie für Informationen über den Zugriff auf die TKLM-Dokumentation den Abschnitt „Dokumentation und Referenzmaterialien“ der Datei **ReadThisFirst.txt** auf dem EKM 3.0-Installationsdatenträger.

Bekannte Probleme und Lösungen

Problem: Ich kann keine Sicherung erstellen.

Beschreibung:

Versuchen Sie, unter Verwendung von Internet Explorer eine Sicherung des Keystores zu erstellen. Wenn Sie ein Sicherungsverzeichnis angeben, das nicht vorhanden ist, wird die Sicherung nicht erstellt.

Lösung:

Führen Sie eine der folgenden Maßnahmen aus. Wenn die von Ihnen versuchte Maßnahme nicht funktioniert, dann führen Sie eine andere aufgeführte Maßnahme durch:

- Aktivieren Sie in Ihrem Browser JavaScript. Wenn Sie Internet Explorer V8 verwenden, dann schalten Sie den Kompatibilitätsansichtsmodus ein.
- Verwenden Sie einen anderen unterstützten Browser. Beziehen Sie sich auf Hardware- und Softwareanforderungen, um weitere Informationen zu erhalten.
- Geben Sie einen Ordner an, der vorhanden ist. Wenn Sie einen neuen Ordner angeben wollen, dann erstellen Sie den Ordner, bevor Sie die Sicherung erstellen.

Problem: Es werden mehrere Sicherungen auf einmal erstellt.

Beschreibung:

Wenn Sie versuchen, eine Sicherung des Keystores zu erstellen, werden mehrere Sicherungsdateien zur gleichen Zeit erstellt. Dieses Problem tritt selten auf.

Lösung:

Alle Sicherungsdateien haben den gleichen Inhalt. Sie können für den Wiederherstellungsvorgang jede beliebige Sicherungsdatei verwenden.

Problem: Ich muss meine Anmeldeinformationen zweimal eingeben.

Beschreibung:

Nach der Zeitüberschreitung von EKM 3.0 (nach einer Leerlaufzeit von etwa 30 Minuten), wird der erste Versuch, sich wieder in EKM 3.0 anzumelden abgelehnt, und Sie müssen sich ein zweites Mal anmelden.

Lösung:

Geben Sie beide Male Ihre EKM 3.0-Anmeldeinformationen an.

Problem: Der rechte Fensterbereich wird durch den Navigationsfensterbereich teilweise verdeckt.

Beschreibung:

Sie verwenden Internet Explorer. Sie greifen auf den EKM 3.0-Bildschirm **Schlüssel- und Geräteverwaltung** zu. Sie wählen entweder die Schlüsselgruppe oder ein Bandlaufwerk aus. Der rechte Fensterbereich wird durch den Navigationsfensterbereich teilweise verdeckt.

Lösung:

Führen Sie einen der folgenden Vorgänge aus:

- Aktualisieren Sie die Bildschirmanzeige.
- Maximieren Sie den Browser.
- Verwenden Sie einen anderen unterstützten Browser. Beziehen Sie sich auf Hardware- und Softwareanforderungen, um weitere Informationen zu erhalten.

Problem: Oben im Browser wird „Zertifikatfehler“ angezeigt.

Beschreibung:

Sie verwenden Internet Explorer 8 im Kompatibilitätsansichtsmodus. Sie importieren erfolgreich ein Echtheitszertifikat, es wird jedoch oben im Bildschirm neben der URL-Leiste **Zertifikatfehler** angezeigt.

Lösung:

Führen Sie einen der folgenden Vorgänge aus:

- Ignorieren Sie den Fehler. Dieser Fehler hat keinen Einfluss auf die Leistung von EKM 3.0.
- Verwenden Sie einen anderen unterstützten Browser (z.B. Internet Explorer 6.X oder Firefox). Beziehen Sie sich auf Hardware- und Softwareanforderungen.

Problem: Ich kann Informationen in Tabellen nicht sortieren.

Beschreibung:

Durch das Verwenden der Felder „Filtern“ oben in den Tabellen der Bildschirme **Serverzertifikate verwalten**, **Sichern und Wiederherstellen** und **Anmeldeinformationsspeicher** werden die Elemente in den Tabellen nicht sortiert.

Lösung:

Klicken Sie in die Überschriftenzeile jeder Spalte, um die Elemente zu sortieren.

Problem: Ich kann keine Beschreibung der Sicherung eingeben, die ich erstellt habe.

Beschreibung:

Sie erzeugen während der Verwendung von Firefox in Windows eine Sicherung. Sie sind nicht in der Lage, eine Beschreibung der Sicherung einzugeben und es wird eine Standardbeschreibung verwendet.

Lösung:

Verwenden Sie eine unterstützte Version von Internet Explorer. Beziehen Sie sich auf Hardware- und Softwareanforderungen, um weitere Informationen zu erhalten.

Problem: Einige Vorgänge in der EKM 3.0 GUI haben zur Folge, dass Scripting-Fehler im Browser als Popup-Meldungen angezeigt werden.

Beschreibung

Im Browser werden Scripting-Fehler angezeigt und die angeforderte Maßnahme wird nicht abgeschlossen.

Lösung:

Führen Sie einen der folgenden Maßnahmen aus. Wenn die von Ihnen versuchte Maßnahme nicht funktioniert, dann versuchen Sie eine andere:

- Aktivieren Sie in Ihrem Browser JavaScript. Wenn Sie Internet Explorer V8 verwenden, dann schalten Sie den Kompatibilitätsansichtsmodus ein.

ANMERKUNG: Sie müssen nach der Anmeldung an EKM 3.0 den Kompatibilitätsansichtsmodus aktivieren.

- Verwenden Sie einen anderen unterstützten Browser. Beziehen Sie sich auf Hardware- und Softwareanforderungen, um weitere Informationen zu erhalten.

Problem: Während der Deinstallation zeigt die Fortschrittsleiste den Fortschritt nicht genau an.

Beschreibung

Die Deinstallationsfortschrittssleiste zeigt den Fortschritt nicht genau an. Die Leiste springt zu Beginn der Deinstallation auf ungefähr 30% und bleibt während der Dauer der Deinstallation dort. Am Ende bewegt sie sich auf 100%.

Lösung:

Dies ist ein bekanntes Problem, das nicht auf ein Problem mit der Deinstallation hinweist.

VORSICHT: Starten Sie das System nicht neu und brechen Sie die Deinstallation nicht ab.

Problem: Die Einstellungen für den Bildschirm „Schlüssel- und Geräteverwaltung“ wirken sich nicht aus.

Beschreibung

Wenn ich im Bildschirm „Schlüssel- und Geräteverwaltung“ die Einstellungen für die Laufwerkskommunikation ändere, wirkt sich die Änderung nicht aus.

Lösung:

Stoppen und starten Sie den EKM 3.0 Server, nachdem Sie die Einstellung für die Laufwerkskommunikation geändert haben. Die Änderungen werden sich auswirken. Beziehen Sie sich auf Starten und Stoppen des EKM 3.0 Servers in Windows oder Starten und Stoppen des EKM 3.0 Servers in Linux, um weitere Informationen zu erhalten.

Problem: Auf einem Windows 2008-Server zeigt die Taskleiste nach Fertigstellung der Installation des EKM 3.0 ein grünes, dem Installationsverfahren zugehöriges Symbol an.

Beschreibung

Die Taskleiste zeigt ein grünes Symbol an.

Lösung:

Dies ist ein bekanntes Problem, das sich nicht auf den Funktionsumfang oder die Zuverlässigkeit von EKM 3.0 auswirkt. Wenn Sie sich vom System abmelden und wieder anmelden, wird das Symbol nicht angezeigt.

Problem: Beim Konfigurieren der Installation von EKM 3.0 zeigen einige Felder eine „0” an.

Beschreibung

Beim Konfigurieren der Installation von EKM 3.0 zeigen einige Felder eine „0” an. Dies tritt auf, wenn Sie beim Installieren von EKM 3.0 ein Installationsprofil verwenden, das entweder ungültig ist oder fehlende Felder aufweist.

Lösung:

Vergewissern Sie sich, dass Sie ein gültiges Installationsprofil verwenden.

ANMERKUNG: Wenn Sie die Felder manuell ausfüllen, müssen sie sicherstellen, dass die Daten exakt mit der ursprünglichen Installation übereinstimmen, anderenfalls kann der zweite Server nicht als Backup-Server für den ersten Server verwendet werden.

Problem: Beim Erstellen einer Sicherung wird die Fehlermeldung „Softwarefehler“angezeigt.

Beschreibung

Sie erhalten beim Erstellen einer Sicherung eine Fehlermleldung, die besagt, dass ein Softwarefehler vorliegt.

Lösung:

EKM 3.0 hat auf Servern mit 24 oder mehr CPUs eine bekannte Einschränkung. Sie müssen das aktuellste universelle Fehlerbehebungpaket für DB2 installieren, um das Problem zu beheben.

ANMERKUNG: Beziehen Sie sich für weitere Informationen auf die Versionshinweise auf: **support.dell.com/manuals**. Navigieren Sie auf **Software → Systemverwaltung → Dell Encryption Key Manager** .

Problem: Ich kann zu einem neu erstellten Benutzer bei Verwendung von Internet Explorer V8 keine Rollen hinzufügen.

Beschreibung

Wenn Sie sich als EKM 3.0-Administrator anmelden, einen neuen Benutzer erstellen und anschließend versuchen, eine Rolle zum neu erstellten Benutzer hinzuzufügen, wird eine JavaScript-Fehlermeldung angezeigt und die Rolle wird nicht hinzugefügt.

Lösung:

Erstellen Sie zuerst den Benutzer, fügen Sie anschließend unter Verwendung des Bildschirms **Administratorbenutzerrollen** Rollen zum Benutzer hinzu. Navigieren Sie für den Zugriff auf diesen Bildschirm im Navigationsfensterbereich zu **Benutzer und GruppenAdministratorbenutzerrollen**. Sie können dieses Problem auch lösen, indem Sie eine unterstützte Version von Firefox verwenden.

Problem: Wenn ich EKM 3.0 deinstalliere, wird die Java-Fehlermeldung „Stapelüberlaufausnahme” angezeigt.

Beschreibung

Wenn Sie EKM 3.0 deinstallieren, wird eine Java-Fehlermeldung angezeigt.

Lösung:

Deinstallieren Sie EKM 3.0 manuell. Beziehen Sie sich auf EKM 3.0 - Manuelle Deinstallation, um weitere Informationen zu erhalten.

Problem: Der EKM 3.0 Deinstallationsvorgang wird für mehrere Stunden ausgeführt und wird nicht abgeschlossen.

Beschreibung

Wenn Sie versuchen, EKM 3.0 zu deinstallieren, wird die Deinstallation nicht abgeschlossen.

Lösung:

Deinstallieren Sie EKM 3.0 manuell. Beziehen Sie sich auf EKM 3.0 - Manuelle Deinstallation, um weitere Informationen zu erhalten.

Installieren der compat-libstdc++ Library

Die Library **compat-libstdc++-33-3.2.3-61** oder höher muss vor dem Installieren von EKM 3.0 auf Linuxplattformen installiert sein.

Wenn Sie beim Installieren von EKM 3.0 auf Linux den folgenden Fehler erhalten, müssen Sie **compat-libstdc++** installieren:

```
Auf Ihrem Betriebssystem ist das compat-libstdc++ Paket nicht installiert.
```

So installieren Sie **compat-libstdc++**:

1. Navigieren Sie in einer Terminalsitzung zur RPM-Datei **compat-libstdc++** im Ordner **EKMPREREQLIBS** auf dem EKM 3.0 Installationsdatenträger, indem Sie den folgenden Befehl geben:
   `cd /<path_to_EKM_3.0_installation_dvd>/EKMPREREQLIBS`
2. Installieren Sie **compat-libstdc++,** indem Sie den folgenden Befehl geben:
   `rpm -ivh compat-libstdc++*.rpm`

ANMERKUNG: Wenn eine Fehlermeldung angezeigt wird, die besagt, dass das **compat-libstdc++** RPM, das Sie zu installieren versuchen einen Konflikt mit dem bereits installierten **libstdc++-33** aufweist, dann führen Sie die folgenden Schritte durch:

a. Geben Sie den folgenden Befehl:
   `rpm –e libstdc++-33`
b. Geben Sie den folgenden Befehl:
   `rpm -ivh compat-libstdc++*.rpm`